THINK AHEAD

2024

REPORT

THINK AHEAD, ACT NOW.

Annual Report

NEOSECURE
By SEK Security Ecosystem Knowledge

Sobre
Neosecure by SEK

En un ecosistema que combina las mejores tecnologías, ofertas de servicios y un equipo de profesionales altamente capacitados, contamos con el conocimiento y la capacidad para enfrentar los más diversos desafíos de ciberseguridad.

NeoSecure by SEK integra el ecosistema de SEK con más de 20 años de experiencia, + de 1.000 colaboradores y una base de +800 clientes en la región, operamos en los mercados de Brasil, Chile, Argentina, Colombia y Perú, donde contamos con tres Cyber Defense Center y dos Cyber Response Center, además de centros avanzados de investigación en los Estados Unidos y Portugal.

Ayudamos empresas de los más diversos sectores a hacer frente a ciber amenazas complejas a lo largo de su jornada de ciberseguridad – actuando ahora y mirando hacia el futuro.

Un mundo en **maduración**

La evolución de la ciberseguridad es un fenómeno que algunas veces se da de una forma incremental, sin grandes sorpresas y mostrando variantes y reafirmaciones de las tendencias que ya se observaban los años anteriores, mientras que otras veces presenta saltos inesperados. Ocasionalmente, algún fenómeno remueve los cimientos del medio, haciendo que el énfasis cambie bruscamente y genere una explosión de innovación.

En el pasado, el ataque a Lockheed Martin, dio lugar al desarrollo del cyber kill chain, la aparición de malwares sofisticados como Stuxnet y otros impulsaron la aparición de nuevos sistemas antimalware como los sandbox, el desarrollo del ransomware, los APT y en general, los ataques dirigidos, impulsaron a los sistemas de EDR y otros mecanismos de detección.

El año 2022 tuvo a la explosión de las Inteligencias Artificiales Generativas como elemento de disrupción central.

Durante el año 2023, no hubo nada parecido a esos momentos transformadores, pero si la maduración de fenómenos que ya habíamos vislumbrado. El desarrollo de las IA Generativas, generan una serie de efectos, como la prevención del deepfake o la protección de la misma infraestructura y sistemas de IA.

Por otro lado, la relevancia que ha tomado la disciplina de ciberseguridad, manifestada en el crecimiento de los presupuestos y la vitalidad del entorno de inversión de riesgo, la van moviendo de su espacio eminentemente técnico a uno de alienación con el negocio y de gestión adecuada de los recursos.

Por otro lado, el surgimiento de cientos de tecnologías y temáticas que abruman a los responsables del área, han tenido como efecto una tendencia hacia la consolidación. La adopción de plataformas tecnológicas altamente integradas es una de ellas, pero la integración de temáticas es otro. Así, por ejemplo, diversas prácticas relacionadas con la exposición, como la gestión de vulnerabilidades, pentesting, gestión de postura, se van consolidado en torno al concepto de Gestión Continua de la Exposición visto como un fenómeno que debe ser abordado de forma integral.

La identidad es otro espacio que ha tomado sostenidamente un lugar de privilegio y su cuidado enfrenta desafíos relevantes como las mencionadas técnicas de deepfake, entre otras.

La búsqueda de mejores estrategias de protección se hace indispensable y nuevos modelos como ZeroTrust, ponen un énfasis especial en la identidad como elemento central.

Si bien no ha sido un año de acontecimientos explosivos dentro de la industria, lo que ha ido aconteciendo, permite prever una serie de caminos interesantes y no carentes de desafío, orientados a construir mejores capacidades en una gestión cada vez más cerca del negocio.

Acerca de los datos

Este reporte que afecta a los sectores de TI y OT para el año 2023 considera, como fuente de datos, diversas fuentes abiertas y privadas, así como los propios datos del SOC de NeoSecure by SEK.

Los datos regionales incluyen los países donde NeoSecure by SEK mantiene sus operaciones: Argentina, Brasil, Colombia, Chile y Perú.

Para efecto de los datos de exposición, hemos utilizado los ejercicios de pentesting de nuestros equipos de seguridad ofensiva, nuestros equipos consultivos, nuestros servicios de Cloud Security Posture Management y fuentes públicas.

Además, se hace una distinción entre Ransomware y "otras violaciones". Las primeras están relacionadas con ataques realizados por grupos de Ransomware, mientras que las segundas se refieren a ataques realizados por grupos APT para otros fines (espionaje, hacktivismo, robo de propiedad intelectual, etc.).

PERÍODO DE ANÁLISIS

2023

ALERTAS ANALIZADAS

+1.535.000

FUENTES ABIERTAS

8

ALERTAS ANALIZADAS

1129

EJERCICIOS DE REDTEAM EJECUTADOS

15 años de experiencia

805

ORGANIZACIONES EVALUADAS EN CLOUD

148

Índice

06 **TENDENCIAS** DE LA AMENAZA

07 Con menos espectacularidad, la amenaza se expande

08 Grandes tendencias en la amenaza

12 Brechas

17 Actores de Amenaza

29 Mirada desde el monitoreo de seguridad

36 Conclusiones

37 **TENDENCIAS** DE LA EXPOCISIÓN

39 Una visión innovadora con el CTEM y cómo podemos harcelo

40 Nuestra visión e índice de Exposición

41 Sector financeiro

42 Manufactura

43 Medios

44 Salud

45 Servicios

46 Retail

47 Principales debilidades

48 Debilidades en la Nube

49 Conclusiones y recomendaciones

50 **TENDENCIAS** DE LA INDUSTRIA

51 Deepfake, cuando nos robaron el rostro

54 IA también es un sistema a ser protegido

57 Automatización, más allá del SOAR

59 Seguridad de la Identidad, no sólo prevenir, también detectar

62 Más allá de la gestión de vulnerabilidades: La Gestión Continua de la Exposición

65 El Next Generation CISO

68 Conclusiones finales

69 **NUESTRA VISIÓN**

70 Producutos y Servicios

71 NeoSecure by SEK

TENDENCIAS
DE LA AMENAZA

Con menos espectacularidad, la amenaza se expande

El año 2023, desde la perspectiva de la amenaza ha sido un año que ha carecido de la espectacularidad de otros. No tuvimos un Stuxnet, ni la devastación que provocó el NotPetya, o un APT como el que sufriera Lockheed Martin en la primera década del siglo. Eso no lo hizo sin embargo un año seguro. La presencia del ransomware se ha hecho casi endémica, y hemos visto como se consolida la idea de la normalización de la amenaza y se convierte en un hecho cotidiano, algo a lo que habría que acostumbrarse.

Tal vez ese acostumbramiento y la larga lista de fronteras superadas hace que lo novedoso lo tenga más difícil: ya vimos en años anteriores el primer hacking satelital, disrupción de sistemas de energía, combustible y agua potable, muertes como consecuencias de un ataque, grandes apagones, peaks de teras de tráfico de denegación y varios otros. Lograr el siguiente hit requiere un esfuerzo importante. Para salvar esa sensación de novedad y este año, podemos citar los primeros ataques de deepfake, algo que seguramente vamos a comenzar a escuchar con mucha más frecuencia.

Naturalmente aparece la pregunta: ¿qué ha pasado con los miles de millones de dólares gastados en nuevas tecnologías, consultorías, servicios, información de inteligencia? ¿Por qué parecen no notarse? No tenemos el contrafactual de esta reflexión y no sabemos cómo sería el escenario actual sin todo ese esfuerzo.

Es posible que el hecho de que podamos seguir funcionando como sociedad sea la respuesta, un "imaginen si no estuviese todo eso".

Pero la verdad es que quienes son hoy responsables de proteger a sus organizaciones, tienen un desafío cada vez más difícil. Las superficies de ataque crecen, los ambientes cambian, los grupos de cibercrimen aumenta y se sofistican y por otro lado, una serie de amenazas que eran pan de todos los días como los ataques a los sistemas SWIFT, los robos masivos de tarjetas de crédito han desaparecido de las portadas.

Debemos entender también, que pese al notable desarrollo tecnológico, el ser humano no siempre sigue ese paso a la misma velocidad. La conocida escasez de profesionales es un punto central, que lleva a otro fenómeno que es la rotación y estrés de los presupuestos.

Desde este escenario cabe preguntarse qué podemos esperar. La respuesta no es muy difícil: más de lo mismo, pero mejor hecho. Condimentado por supuesto con las novedades que el ingenio humano, ahora apoyado por la IA nos pueda entregar. También podemos esperar que el esfuerzo sostenido y profesional de quienes custodian a las organizaciones, los aleje cada vez más de estos escenarios de destrucción de valor.

Grandes tendencias, en la amenaza

Grandes tendencias en la amenaza

Deepfake y el asalto a la identidad

Tal vez el elemento más llamativo con relación a las nuevas técnicas utilizadas por los grupos cibercriminales venga de los ataques denominados de deepfake. La posibilidad de usar la IA para "sintetizar una identidad", es decir tomar a una persona real y producir videos realistas, voces equivalentes y copiar sus tipos de expresiones, son quizá el aspecto más relevante y alarmante en término de amenazas.

Todo esto parece haber tenido el preludio perfecto con la pandemia que aceleró el teletrabajo, haciéndolo parte de la habitualidad. El año 2023 vimos los primeros ejemplos de este tipo de amenazas, con la sintetización de voces de ejecutivos y otros. Las prácticas para robo en escala de imágenes y videos de identidades para luego reproducirlos comienzan a aparecer en el horizonte. Tanto personas como organizaciones sufrirán el asalto de estas nuevas técnicas.

Por supuesto enfrentaremos deepfake de distintas calidades y tendremos a públicos más sensibles de ser engañados que otros. El deepfake se sumará a tendencias anteriores como CEO Fraud, que encontrará acá una nueva vertiente de innovación. La información de videos, fotografías y texto en redes sociales serán un insumo valioso para los atacantes. Esta es una de las amenazas sobre las cuales se deberá tener una especial atención.

Contexto Geopolítico

El contexto geopolítico es más complejo que el de hace un año. Las tensiones en torno a Taiwán, la situación en Gaza, la acción de grupos terroristas en el estrecho de Ormuz, la situación de Ucrania y el potencial alejamiento de EEUU como soporte militar de esta última, han generado un escenario como no se veía hace tiempo. Incluso la región, en general pacífica, vio surgir la amenaza de una posible invasión de Venezuela sobre Surinam. Todas estas situaciones han estado rodeadas de una prolífica actividad de grupos activistas y patrocinados por los estados o grupos en disputa.

Las acciones de espionaje, de sabotaje, de desinformación sin contar con las acciones operativas como parte de los mismos enfrentamientos ha aumentado de manera sensible . Para esto, los estados recurren a sus propios equipos, pero muchas veces, recurren a grupos ciberciminales con los que forman alianzas. Filtraciones obtenidas por grupos pro-rusos de militares alemanes respecto al uso de misiles, ataques de grupos pro-palestinos a empresas israelíes, aumento de la actividad originada en China contra organizaciones norteamericanas son una pequeña muestra del catálogo de actividad en torno a estos conflictos.

Esta actividad tiene varios efectos colaterales. El primer tipo de efectos dice relación con el trasvasije de técnicas y también actores desde el mundo de la acción estatal al mundo de cibercrimen, lo que va haciendo la acción de estos últimos más efectiva y profesional.

El segundo efecto, son las acciones que escapan de control. Tal fue el caso de NotPetya, una acción dirigida por los servicios secretos rusos contra Ucrania, que resultó en un gusano que detuvo infraestructura a través del planeta en tiempos record y con costos de más de USD 10 billones.

Los responsables de ciberseguridad deberemos estar preparados para escenarios inesperados, interrupción de infraestructura y deberán ampliar su capacidad de inteligencia para evaluar bien estos posibles escenarios.

I.A (Inteligencia Artificial)

El uso de las capacidades de IA para aumentar el potencial de la amenaza ha comenzado a dar sus primeros pasos. Un caso interesante es el del modelo Llama 2 desarrollado por Meta, el que fue puesto primero filtrado y luego de dominio público por la propia empresa. Crowdsitrke habría encontrado evidencia de su uso en la creación de los Power Shell de algunos ataques.

Si bien la evidencia del uso de IA en la ejecución misma de los ataques ha sido baja, no podemos descartar que durante el 2024 comiencen a aparecer algún tipo de toolkit orientado a esta actividad, aunque los más probable es que esté orientado a ser un sistema de auxilio al atacante, sugiriendo los pasos a seguir y no ejecutándolos. En la medida que la confianza de los actores sobre estas herramientas crezca, recién comenzaremos a ver los primeros casos de ejecución automatizada.

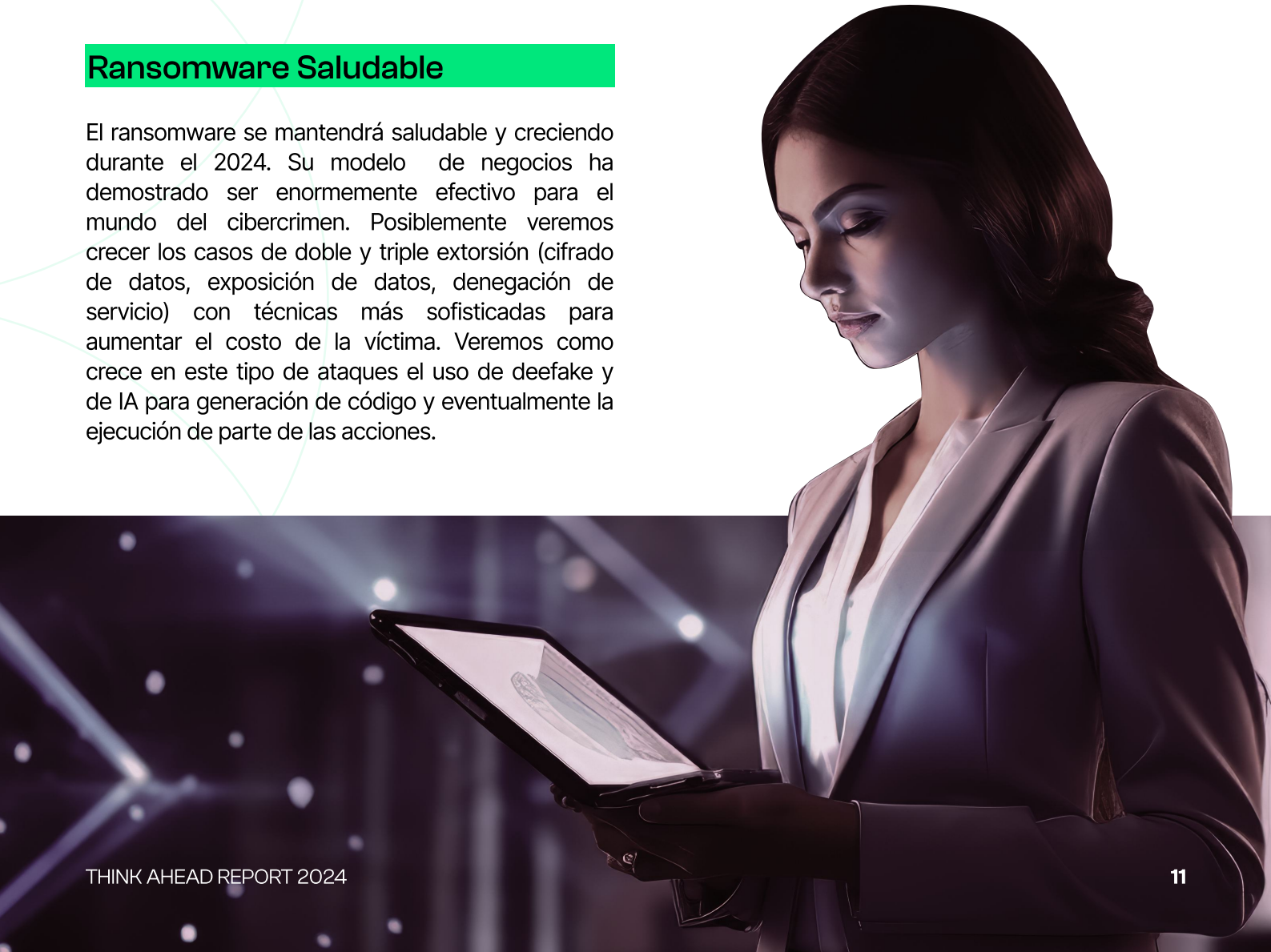
Ransomware Saludable

El ransomware se mantendrá saludable y creciendo durante el 2024. Su modelo de negocios ha demostrado ser enormemente efectivo para el mundo del cibercrimen. Posiblemente veremos crecer los casos de doble y triple extorsión (cifrado de datos, exposición de datos, denegación de servicio) con técnicas más sofisticadas para aumentar el costo de la víctima. Veremos como crece en este tipo de ataques el uso de deefake y de IA para generación de código y eventualmente la ejecución de parte de las acciones.

WiFi e IoT

El ataque a los dispositivos IoT se encuentra en la retina de la industria desde hace un tiempo y la proliferación de estos sistemas con los problemas de securización, crea un escenario de riesgo importante. El ataque a los sistemas de IoT se está viendo complementado por el uso de las redes WiFi poco protegidas para acceder al interior de la red.

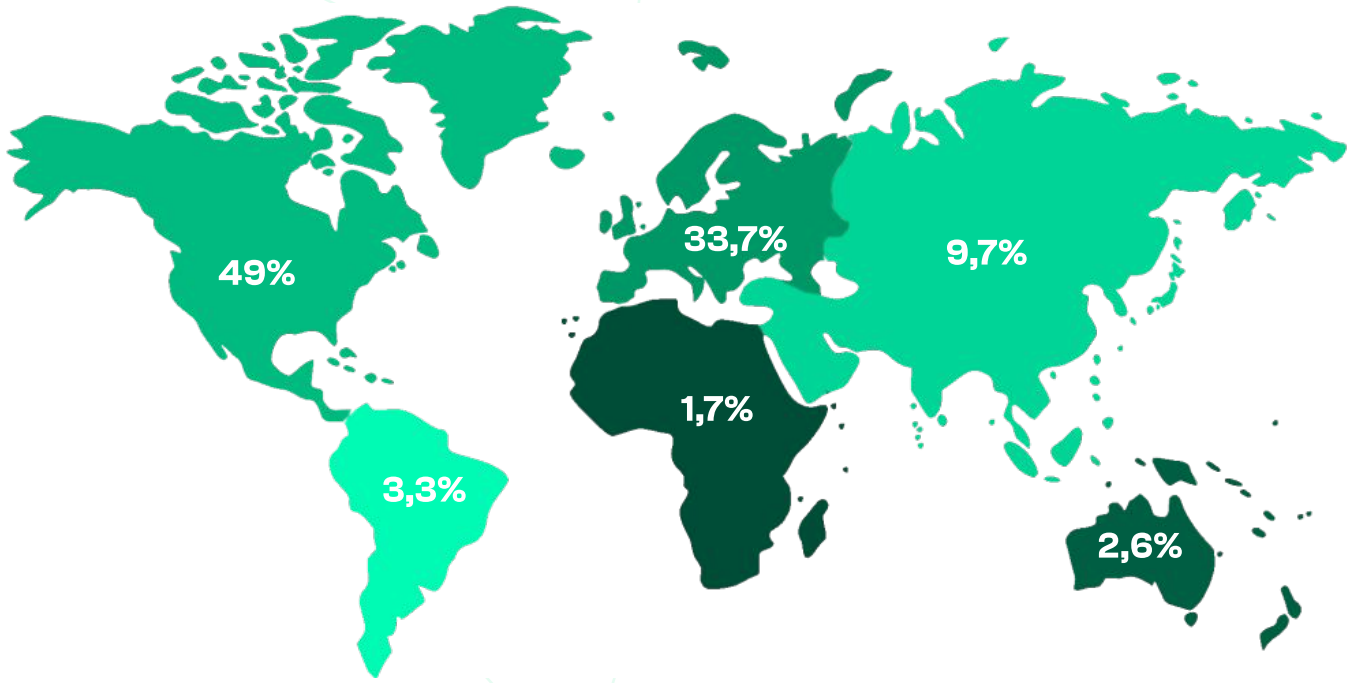
La combinación de, por ejemplo, una red WiFi que expone un sistema de aire acondicionado inseguro, generan una ampliación de la superficie de ataque, posibilitando el acceso a actores maliciosos.
Por otro lado, la endémica incapacidad de asegurar estos dispositivos o de ponerlos en redes segmentadas facilitan el movimiento lateral. Al no contar con inventarios completos, los equipos responsables de ciberseguridad, tienen baja visibilidad y por tanto, un alto riesgo.



Brechas

Brechas

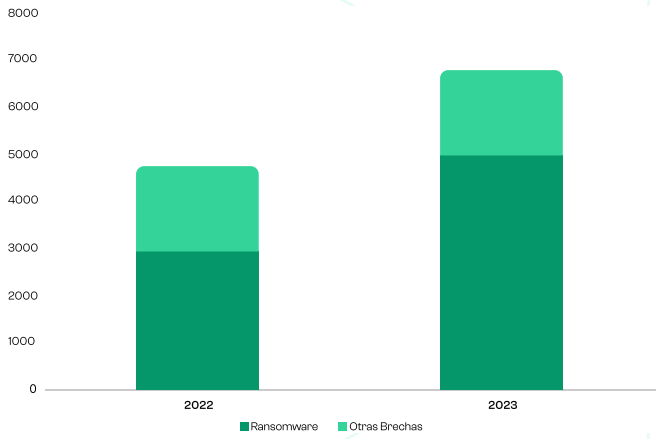
Brechas Nivel Global



En el 2023, un 73% de las brechas correspondieron a ransomware. Aproximadamente un 3,3% de la actividad se encontró en Sudamérica. Esta cifra es menor a lo observado en otros años y puede deberse al recrudecimiento de actividad en otras regiones por cuestiones geopolíticas

Fuente: información pública y registros del DBIR

Brechas nivel global comparativa 2022 vs 2023



Nota: Datos corresponden a todo el 2022 y enero a septiembre 2023

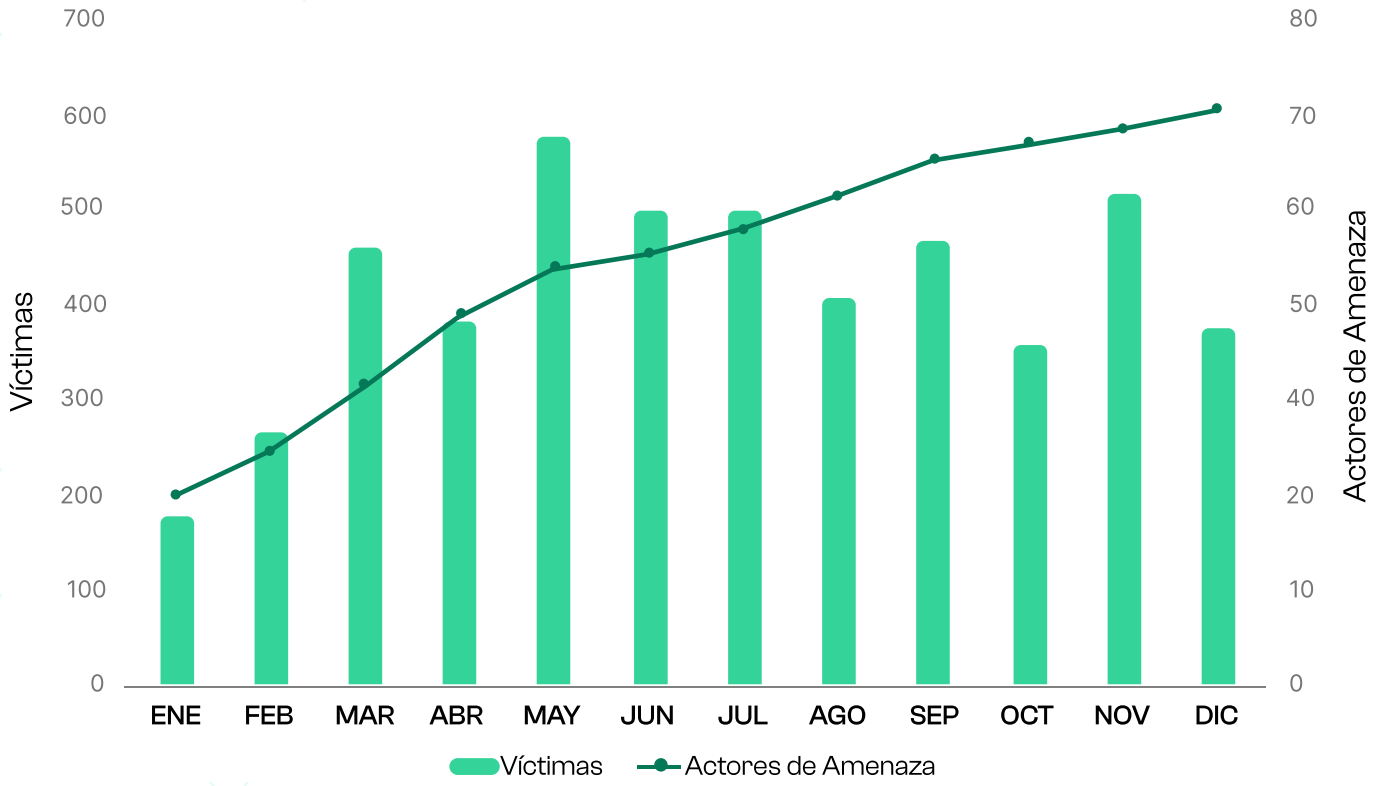
Fuente: información pública y registros del DBIR

Durante el año 2023 se observó un aumento de 43,74% en brechas con respecto al 2022. Este aumento se debió principalemente al aumento del Ransomware que creció en un 71% con respecto al año 2022

La efectividad del modelo de negocios del ransomware es una explicación de porqué esta modalidad ha crecido de esta forma

Otros tipos de brechas mantuvieron la misma tendencia en los últimos 2 años.

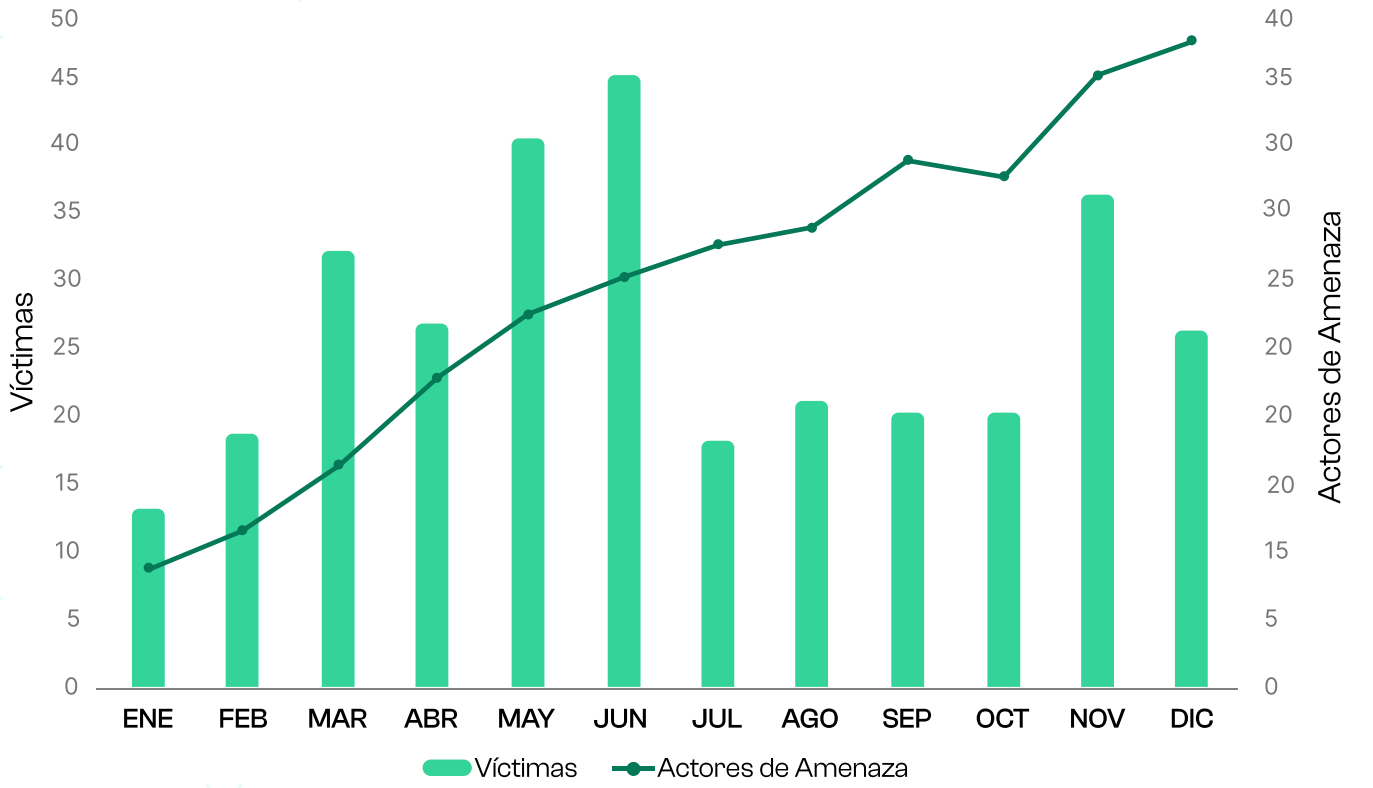
Brechas nivel global Ransomware



En mayo el actor de amenaza Cl0p aprovecha la vulnerabilidad de MOVEit lo que deriva en un peak de actividad cibercriminal. Los actores de amenazas relacionados con Ransomware se incrementaron en más del 200% atraidos por lo atractivo del modelo de negocios. Este crecimiento de actores explica el crecimiento del ransomware como principal amenaza.

El crecimiento en la cantidad de actores permite predecir un aumento de la actividad de este tipo de amenazas. La diversidad de actores se manifestará en una variedad de técncias más amplia, lo que hará más compleja la acción de protección. Se estima que la desarticulación de grupos de cibercrimen ocurrida durante 2023, generó una proliferación de emprendimientos por parte de aquellos miembros que no pudieron ser capturados

Brechas en Latinoamérica Ransomware



Los actores de amenazas asociados a Ransomware, que han atacado en la región ha aumentado un 443% lo que indica que la región es vista como un terreno fértil para este tipo de operaciones

La tendencia de ataques se mantiene en la región, exceptuando en los meses de mayo y junio, por la explotación de la vulnerabilidad de MOVEit por parte de Cl0p. La actividad asociada al ransomware ha impactado a un conjunto heterogéneo de organizaciones en diversas industrias como energía, comercio electrónico y otras.

Es especialmente llamativo, el impacto a la cadena de suministros, sobre todo a proveedores de telecomunicaciones y servicios de datacenters. El efecto en cadena generado por estos ataques implica una presión adicional hacia el afectado por sus propios clientes. También posibilitan al actor el acceso a los datos y sistemas alojados en los datacenter. El crecimiento en la cantidad de actores permite predecir un aumento de la actividad de este tipo de amenazas. La diversidad de actores se manifestará en una variedad de técncias más amplia, lo que hará más compleja la acción de protección.

Brechas por Ransomware en Latinoamérica

Total Actor	Bolivia	Martinique	Paraguay	Haiti	Nicaragua	Ecuador	Cuba	Dominican Republic	Uruguay	Costa Rica	Panama	Venezuela	Guatemala	Peru	Chile	Colombia	Argentina	Mexico	Brazil	País / Actor
76			1	1	1	1			2	2	2	2	3	6	4	6	6	18	21	LockBit
39	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	4	27	8BASE
25				1				2			1	1	1		3		2	6	2	Alphv (BlackCat)
14	1							1		1					3	2	3	1	2	Medusa
10													1		1	3	1	3	1	CLOP
9							3										1	1	4	STORMOUS
8					1						2						2	1	2	Akira
7										1						2		3	1	NoEscape
7		1						1							1		1	1	2	Rhysida
7									1						1		1		4	Knight
4																1	3			Qilin
4												1						2	1	Royal
3									1									1	1	Cactus
3																			3	Ransomed
3																	2	1		LostTrust Team
3														1					2	Mallox
3															1			2		BlackByte
2						1										1				Vice Society
2																		1	1	Ragnar Locker
2																		2		PLAY
2																			2	Black Basta
2																	1		1	Trigona
2																1	1			MalasLocker
2																	2			DragonForce
1																		1		Hunters International
1																			1	CrossLock
1									1											AvosLocker
1														1						DarkPower
1								1												RansomHouse
1												1								BlOOdy
1																1				Izis
1																		1		RA Group
1																		1		Cloak
1													1							Cyclops
1																			1	Nokoyawa
1																			1	Dunghill Leak
1																			1	BlackSuit
252	1	1	1	2	2	2	3	5	5	5	5	6	8	10	14	18	27	56	87	Total País

Actores de Amenaza

Actores de Amenaza

Actores regionales

La región cuenta con la presencia de numerosos actores globales que operan en diversos países de la región, algunos más activos que otros. Estos actores pueden estar enfocados en uno u otro país dependiendo de sus propias capacidades.

La región cuenta con un bajo desarrollo de grupos ciber-criminales de nivel global en la industria del ransomware. Hemos provisto aquí un resumen de los principales actores y la actividad de estos dentro de la región, así como sus focos, capacidades e historial.

Brechas por Ransomware en Latinoamérica

País / Actor	LockBit	8BASE	Alphv (BlackCat)	Medusa	CLOP	STORMOUS	Akira	NoEscape	Rhysida	Knight	Qilin	Royal	Cactus	Ransomed	LostTrust Team	Mallox	BlackByte	Vice Society	Ragnar Locker	PLAY	Black Basta	Trigona	MalasLocker	DragonForce	Hunters International	CrossLock	AvosLocker	DarkPower	RansomHouse	BIOOdy	Izis	RA Group	Obak	Cyclops	Nokoyawa	Dunghill Leak	BlackSuit	Total País
Brazil	21	27	2	2	1	4	2	1	2	4		1	1	3		2			1		2	1				1									1	1	1	87
Mexico	18	4	6	1	3	1	1	3	1			2	1		1		2		1	2					1							1	1					56
Argentina	6	1	2	3	1	1	2		1	1	3				2							1	1	2														27
Colombia	6	1		2	3			2			1							1					1								1							18
Chile	4	1	3	3	1				1	1							1																					14
Peru	6	1														1												1										10
Guatemala	3	1	1		1																												1					8
Venezuela	2	1	1									1																		1								6
Panama	2	1	1				2																															5
Costa Rica	2	1		1				1																														5
Uruguay	2	1								1			1														1											5
Dominican Republic		1	2	1					1																				1									5
Cuba		1				3																																3
Ecuador	1	1																1																				2
Nicaragua	1	1					1																															2
Haiti	1	1	1																																			2
Paraguay	1	1																																				1
Martinique		1							1																													1
Bolivia		1		1																																		1
Total Actor	76	39	25	14	10	9	8	7	7	7	4	4	3	3	3	3	3	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	252

No es una sorpresa que la mayoría de las brechas se presenten en los países de mayor tamaño o desarrollo dentro de la región. Esto se deben en parte por su tamaño, en estos países operan ya redes de agentes que conocen bien el medio y están dispuestos a buscar nuevas ofertas de RaaS con mejores condiciones comerciales y mayor posibilidad de éxito.

Aquellos actores más consolidados , son los que cuentan con redes de agentes más sólidas lo que les permite expandirse rápidamente. Esto está asociado a modelos de negocios y tecnologías más atractivos para los agentes

Principales actores en la región

Los principales actores de amenaza son los siguientes:

LockBit:

Es el actor malicioso con la mayor presencia en el mundo y LATAM.

Su objetivo es lograr detener los procesos productivos y la doble extorsión.

Su motivación subyacente es monetaria, por lo que sus ataques son dirigidos a todo tipo de industria.

8Base:

Es el segundo actor malicioso con presencia en LATAM.

Sus principales víctimas se encuentran en EE.UU. Y Brasil.

Utiliza Phishing o credenciales comprometidas para ingresar en las redes de sus víctimas.

BlackCat (ALPHV):

Opera como Ransomware as a Service (Raas)

Sus principales víctimas son el sector servicios legales y servicios IT, salud también empresas que manejan altos volúmenes de información de identificación personal.

Obtienen acceso inicial a través de credenciales o phishing

En general, la motivación principal de los actores en Latinoamérica es de carácter monetario.

No podemos descartar ver alguna actividad de otro tipo (hacktivismo, espionaje) derivada del escenario geopolítco actual.

LockBit

Nombres:

- LockBit
- ABCD
- EvilCorp

Descripción:

- Enfocado en secuestro de datos

Capacidades:

- Acceso inicial a través de servidores expuestos a Internet comprometidos (T1190 - Exploit Public-Facing Application) o cuentas RDP que generalmente son adquiridas u obtenidas a través de afiliados (T1078 - Valid Accounts).
- Explotación de vulnerabilidades de VPN (T1190 - Exploit Public-Facing Application)
- Modificación de GPO en el AD para escalar privilegios (T1484 - Domain Policy Modification).

Víctimas:

- Empresas de rubro manufactura, energía, utilities e infraestructura crítica.

Infraestructura:

- Uso de StealBit para reunir y exfiltrar datos

Impacto:

- Robo de información confidencial

8BASE

Nombres:

- 8Base

Descripción:

- Enfocado en secuestro de datos

Capacidades:

- Uso de malware para desplegar Ransomware de manera ofuscada (SmokeLoader) (T1587.001 - Malware)
- Uso de phishing para obtener acceso a redes corporativas (T1566 - Phishing)

Víctimas:

- Empresas de rubro transporte, Quimicas, Industrias metalúrgicas y utilities

Infraestructura:

- Uso de SystemBC para reunir y exfiltrar datos

Impacto:

- Robo de información confidencial

BlackCat

Nombres:

- Alphv/AlphaVM
- Zirconium

Descripción:

- Enfocado en secuestro de datos

Capacidades:

- Explotación de servidores Exchange vulnerables, aplicativo ConnectWise, RDP expuesto a internet (T1190 - Exploit Public-Facing Application) y credenciales robadas (T1078 - Valid Accounts).
- Extrae credenciales desde estaciones de trabajo y se mueve dentro de la red usando PsExec (T1588.002 – Tool)

Víctimas:

- Empresas de rubro energía, utilities, industria pesada

Infraestructura:

- Uso de ExMatter para reunir y exfiltrar datos

Impacto:

- Robo de información confidencial

Medusa

Nombres:

- Medusa Blog

Descripción:

- Enfocado en secuestro de datos

Capacidades:

- Extorsiona a sus víctimas, amenazando con liberar datos de la compañía si no pagan el rescate de los datos.

Víctimas:

- Empresas de rubro energía, utilities, industria pesada, telecomunicaciones

Infraestructura:

- Desconocida

Impacto:

- Robo de información confidencial

CLOP

Nombres:

- Cl0p
- TA505/FIN11
- Lace Tempest

Descripción:

- Enfocado en secuestro de datos

Capacidades:

- Explotación de vulnerabilidades zero-day (Accellion, SolarWinds, MOVEit) (T1190 - Exploit Public-Facing Application) y phishing para acceder a las redes corporativas (T1566 - Phishing).
- Uso de malware y herramientas de pentesting para persistir y operar en la red interna (Cobalt Strike, SDBOT) (T1588.002 – Tool).

Víctimas:

- Empresas de rubro transporte, Oil & Gas, Utilities

Infraestructura:

- Uso de botnets para propagar malware y mineros de criptomonedas para lavar dinero
- Comprometer aplicaciones usadas en la cadena de suministro

Impacto:

- Robo de información confidencial

Qilin

Nombres:

- Agenda

Descripción:

- Enfocado en secuestro de datos, habitualmente realizando doble extorsión a sus víctimas

Capacidades:

- Uso de phishing y spearphishing para acceder a redes corporativas, junto con la explotación de aplicaciones expuestas a internet como Citrix o RDP
- Uso de credenciales válidas para ingresar a la compañía, conexiones RDP hacia Domain Controllers (T1078 - Valid Accounts).

Víctimas:

- Empresas de infraestructura crítica, educación y salud

Infraestructura:

- Uso de plataforma RaaS
- Uso de servidores Citrix comprometidos para moverse lateralmente por la red

Impacto:

- Robo de información confidencial

STORMOUS

Nombres:

- STORMOUS

Descripción:

- Enfocado en secuentro de datos
- Defacement en sitios expuestos (hacktivismo)

Capacidades:

- Uso de phishing y spearphishing para acceder a redes corporativas, junto con la explotación de aplicaciones expuestas a internet como Citrix o RDP
- Uso de credenciales válidas para ingresar a la compañía, conexiones RDP hacia Domain Controllers (T1078 - Valid Accounts).

Víctimas:

- Empresa alimenticia
- Ministerio de Relaciones Exteriores de un país de Europa del Este

Infraestructura:

- Afiliación con grupo GhostSec

Impacto:

- Robo de información confidencial
- Influencia negativa para la imagen de las compañías afectadas

LostTrust

Nombres:

- LostTrust

Descripción:

- Enfocado en secuestro de datos

Capacidades:

- Utiliza esquema multi-extorsión: cifrado (T1486 - Data Encrypted for Impact), exfiltración (TA0010 – Exfiltration), ataques DDoS (T1584.005 – Botnet) y comunicación con clientes de la organización atacada

- Terminación de procesos críticos: Microsoft Exchange, MSSQL, SharePoint, Tomcat mediante “cmd.exe” (T1489 - Service Stop)

Víctimas:

- Empresas de rubros salud y educación

Infraestructura:

- Payload de ransomware basado en “SFile”

Impacto:

- Robo de información confidencial

Los principales actores de amenaza

Ransomware	T1556 Phishing	T1078 Valid Accounts	T1190 Exploit Public-Facing Application	T1195 Supply Chain Compromise
Lockbit	▲	●	■	–
Medusa	–	–	–	–
8Base	■	■	–	–
BlackCat	▲	●	–	–
ClOp	●	▲	–	■
Qilin	●	–	▲	■
STORMOUS	●	■	▲	–
LostTrust	–	–	–	–

Simbología:

- ● : principal método usado por el actor
- ▲ : segundo método más usado
- ■ : usado en casos aislados, pero es parte del arsenal
- – : sin información

Mirada desde el monitoreo de **seguridad**

Mirada desde el monitoreo de seguridad

El CDC de NeoSecure by SEK preocesa y analiza mensualmento más 35.500 alertas de ciberseguridad en Argentina, Brasil, Chile, Colombia y Perú en más de 150 organizaciones . Estas organizaciones son de variado tipo: finanzas, manufactura, recursos naturales, servicios, salud, seguros, transporte y otros rubros. Dichos eventos provienen de ambientes TI, OT, nube, red interna, perímetro, lo que permite tener una visibilidad bastante completa de lo que sucede en el ambiente.

A través del monitoreo de sistemas perimetrales, como firewall, DNS, Secure Email Gatewys, WAF y otros, incluyendo el monitoreo de sistemas EDR y NDR, el CDC de NeoSecure by SEK, recorre toda la cadena de tácticas de MITRE, lo que le permite tener una visibilidad amplia de las tácticas y técnicas que están siendo utilizadas por los adversarios en la región.

Las alianzas que tiene en inteligencia, con proveedores regionales y globales, le permiten complementar esta mirada con lo que sucede más allá de las fronteras de la organización.

Los datos siguientes son resultado del análisis de dicha información y proveen una mirada interesante y complementaria la entregada por otros referentes globales.

Acceso Inicial (TA0001)

La primera fase se refiere a la información relativa al acceso de los grupos cibercriminales a una organización. Los datos aqui reflejados, corresponden a alertas generadas por nuestros sistemas, la gran mayoría de las cuales no logró éxito en su cometido.

En general, se podrá observar que los actores utilizan un mix de métodos bastante conocidos como phishing, búsqueda de accesos privilegiados, fuerza bruta e intento de explotación de vulnerabilidades.

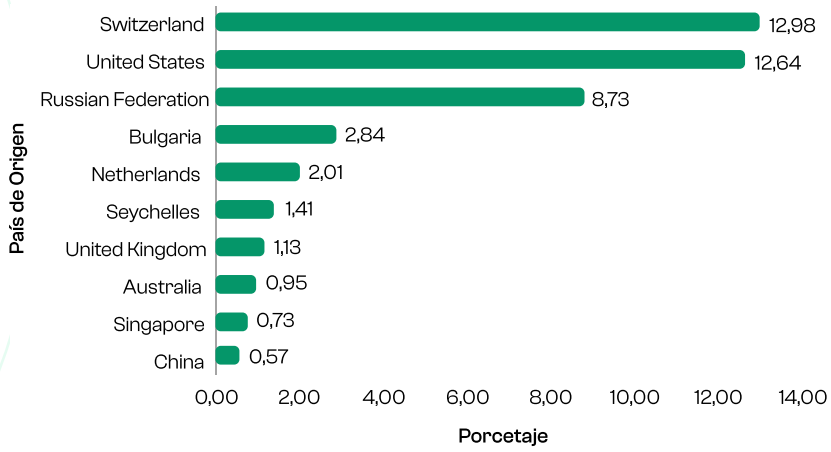
Esta tarea, es generalmente llevada a cabo por bots o por actores especializados en obtener accesos para luego venderlos (Access Brokers). La evidencia encontrada en redes sociales muestra una importante cantidad de credenciales robadas a la venta. Es poco probable que esas credenciales estén asociadas a los ataques observados por NeoSecure by SEK, pues los mecanismos de correlación permiten visualizar cuando el ataque tiene éxito y la acción es bloqueda de inmediato. Sin embargo, si la credencial fue obtenida de otra forma, podríamos encontrar que accesos supuestamente válidos, corresponden a impostores.

Login Fallidos por País Origen - Año 2023

El origen de la actividad indica poco en relación a quién está tras ella. Los actores utilizan una serie de proxys y VPNs o redes de anonimización para que su origen real no sea rastreado.

Pese a eso, países como la Federación Rusia o Bulgaria, presentan una actividad alta. Estos orígenes de cibercrimen asociado y por lo tanto gran parte de las organizaciones tienden a bloquear este tráfico o a investigarlo con más detección.

Esto nos permite inferir que la actividad, sea probablemente debida a bots que están escaneando en busca de accesos

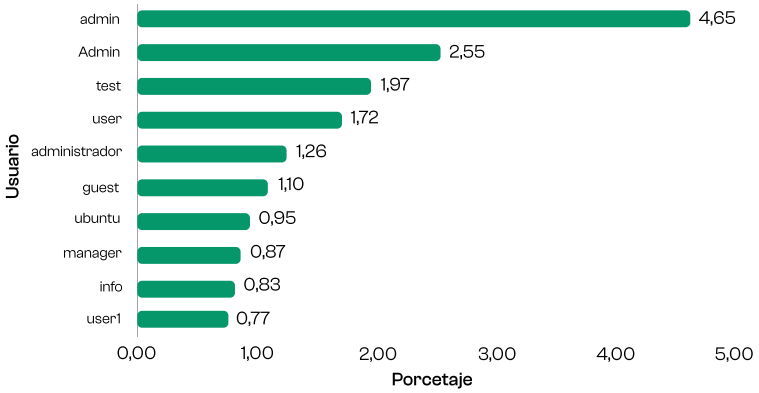


Usuarios afectados por Login Fallidos - Año 2023

En general, una parte importante de los login fallidos se encuentra dirigido a cuentas genéricas.

Si bien son cuentas que podrían estar presentes en diversos sistemas, es esencial entender que pueden ser la entrada a amenazas más importantes como Initial Access Brokers (IABs) y grupos APT.

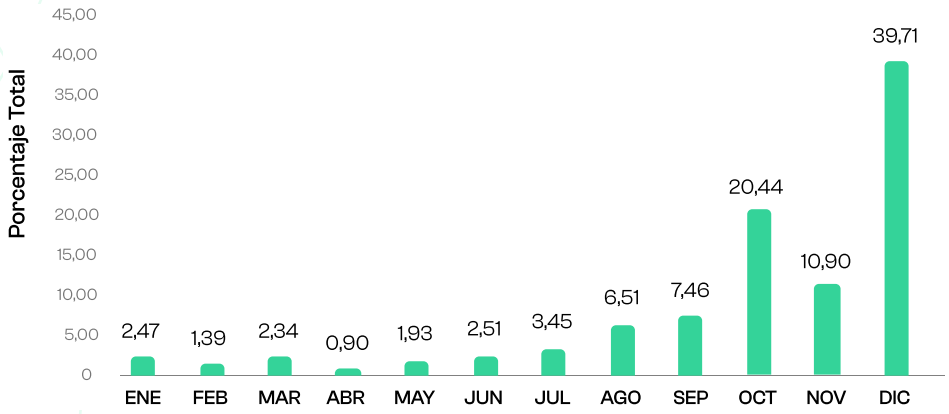
Este tipo de cuentas se prestan, especialmente, para una exploración a través de robots
De no contar con resguardos de seguridad (ej: MFA, políticas de robustez de contraseñas, correcta gestión de cuentas), son un peligro para la confidencialidad de los activos.



Cantidad Login Fallidos - Año 2023

Se aprecia un alza importante en la cantidad total de ataques por fuerza bruta desde Octubre 2023.

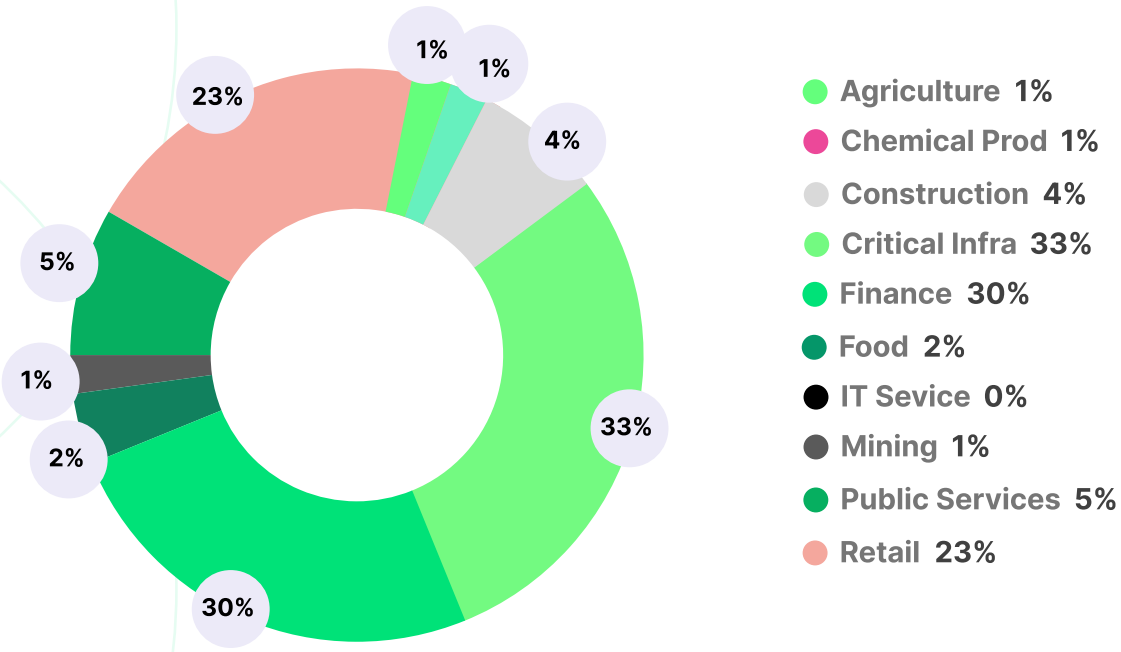
Esto podría ser una percepción de los atacantes de una ausencia de protección de tipo MFA en las cuentas visibles desde Internet



Cantidad Ataques por Industria - Año 2023

Como es de esperar, la industria financiera es la que más ataques de fuerza bruta recibe. La cantidad de intentos se condice con la "magnitud" del botín que guardan las compañías.

La segunda industria más afectada es infraestructura crítica. Considerando que deben cumplir con requisitos de disponibilidad de servicios, pueden tener consecuencias desastrosas en caso de ataque.



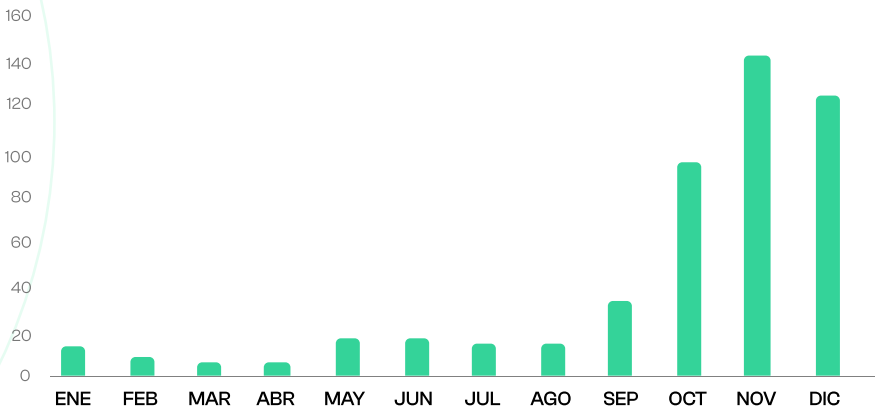
Venta de Credenciales

Total Ventas Credenciales en DarkWeb - Año 2023 - IT/OT

Se observa un aumento significativo en la venta de credenciales a partir de mayo, alcanzando su punto máximo en Noviembre.

Este aumento en las ventas podría tener como consecuencia un incremento en los ataques sufridos por las compañías durante estos meses y los siguientes..

Esto es consistente con el aumento de actores en la región y podría ser preludio de un aumento en los ataques de ransomware durante este año.

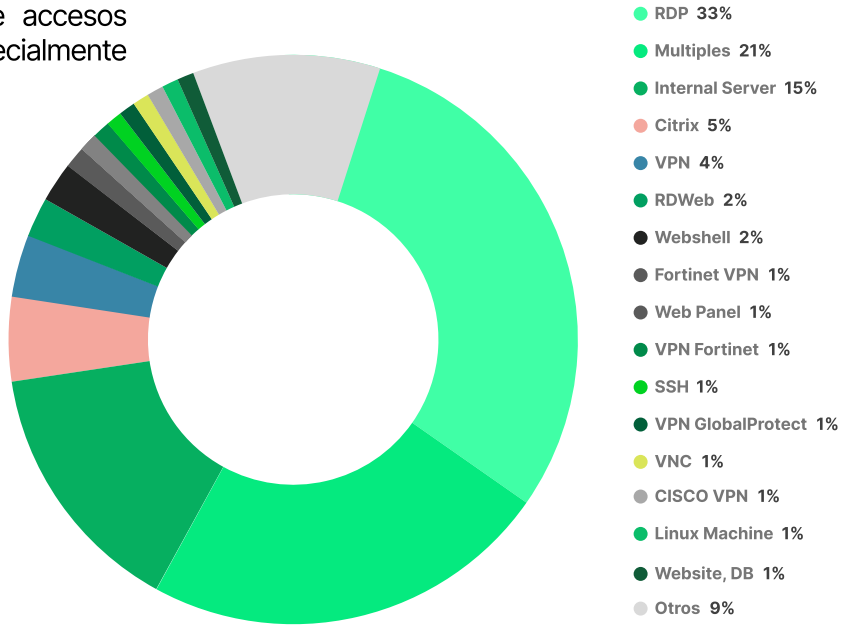


Cantidad de ventas por Tecnología 2023 IT - OT

Resalta la venta de credenciales RDP, lo cual puede atribuirse a la complicada detección de accesos maliciosos a través de este protocolo, especialmente en un contexto de aumento en las conexiones remotas debido al teletrabajo

Este es un tipo de acceso que ha sido utilizado durante un largo tiempo en el medio y no ha perdido su efectividad

El término “múltiples” hace referencia a la venta de más de 1 tecnología (ej: VPN + Webshell, VPN + Citrix, M365 + AnyDesk, etc.).

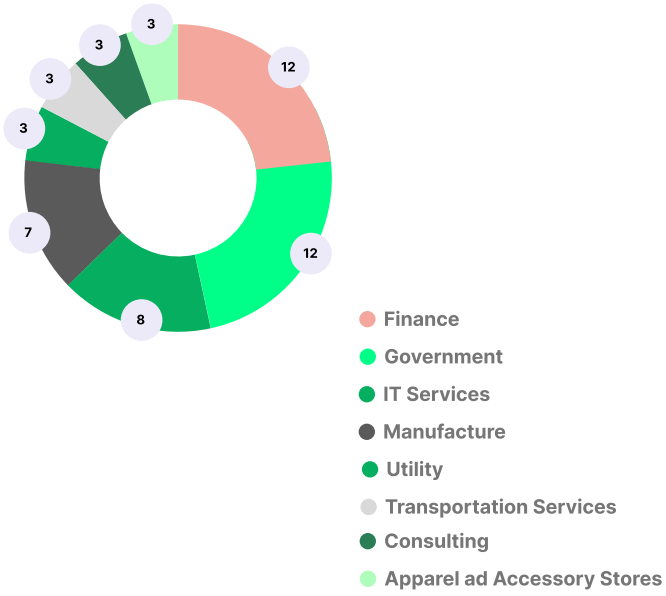


Total de Ventas por Industria en DarkWeb - Año 2023 - IT/OT

El sector financiero se encuentra en la primera línea de riesgo en cuanto a la venta de credenciales. Este fenómeno es congruente con la gran cantidad de recursos financieros que circulan en esta industria, lo que lo convierte en un objetivo tentador para actores maliciosos que buscan obtener beneficios económicos a través de actividades delictivas.

El sector gubernamental es igualmente afectado. Esto podría atribuirse al alto valor estratégico que representa para actores maliciosos, dado su potencial para el espionaje cibernético y la obtención de información sensible.

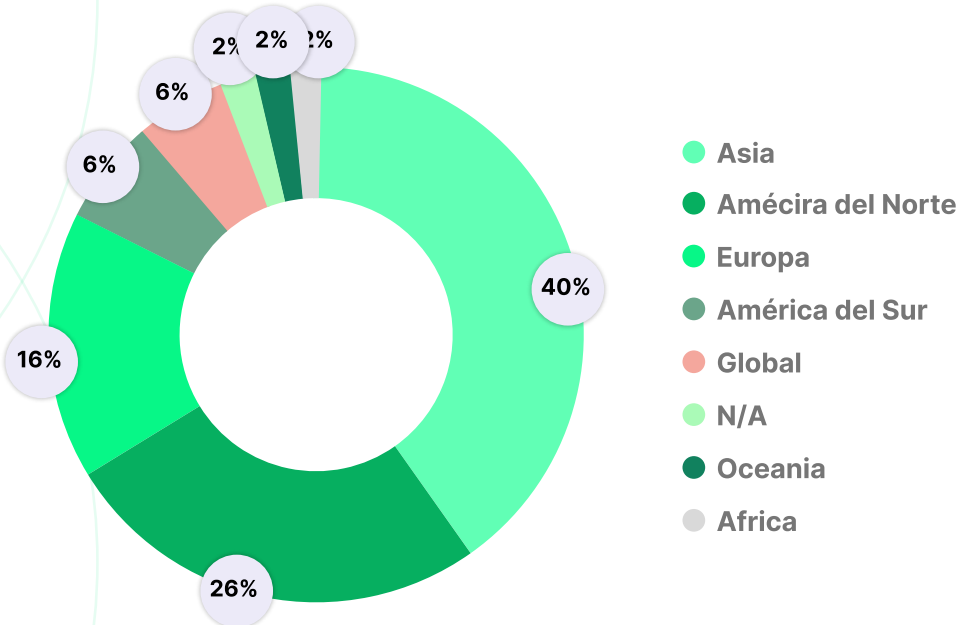
El sector gobierno, presenta una serie de servicios críticos de los cuales depende gran parte de la población, lo que los hace susceptibles a extorsión



Ventas por Continente 2023 IT - OT

Asia y América del Norte ocupan los primeros lugares en la lista de continentes más afectados por la venta de credenciales, respectivamente. Estas regiones se destacan por su densidad empresarial, presencia de potencias económicas y su abundante infraestructura digital. Estos factores hacen que sean blancos particularmente atractivos para cibercriminales en busca de oportunidades para la adquisición y venta de credenciales.

La venta de credenciales en la región es comparativamente más alta que las brechas observadas (3,3 %), lo que podría hablar de una vulnerabilidad relativa mayor



Ejecución (TA0002)

Las técncias de ejecución, son las observadas generalmente en la red interna del cliente y están generalmente asociadas a intentos de ataques de tipo ransomware aunque podrían deberse a otro tipo.

Gran parte de estas técnicas entran en la categoría de LOLBAS (Living-Of-the-Land Binaries, Scripts and Libraries). Su importancia radica en que, debido a que son programas nativos, los actores de amenaza pueden realizar operaciones maliciosas sin llegar a ser detectados.

Su uso implica un alto nivel de sutileza y evasión por parte de los actores de amenaza (podrían pasar por "debajo del radar" sin los adecuados controles de seguridad en activos y equipos de las compañías).

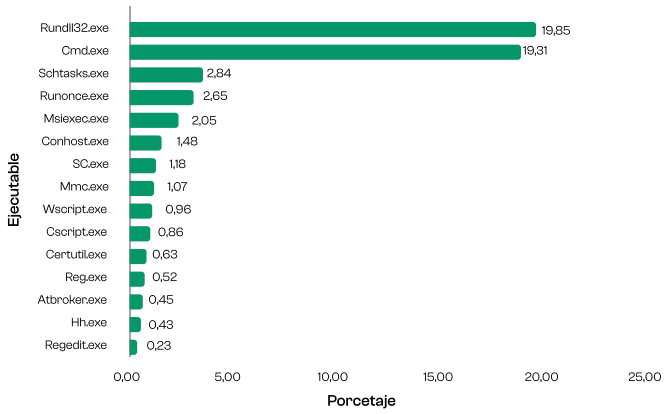
En esta categoría entran ejecutables y bibliotecas nativas de los sistemas operativos, firmados y confiables, que pueden ser utilizados con fines maliciosos y en general han ido reemplazando al malware como herramienta.

Top 15 Lolbas más usados – Año 2023

El uso de "cmd.exe" y "rundll32.exe" lidera entre los LOLBAS. Su uso en instalaciones y configuraciones es común, pero se debe vigilar su uso con argumentos no autorizados.

Mediante acciones de persistencia con "sc.exe" y "runonce.exe", los atacantes instalan servicios o tareas para controlar los equipos según sus objetivos.

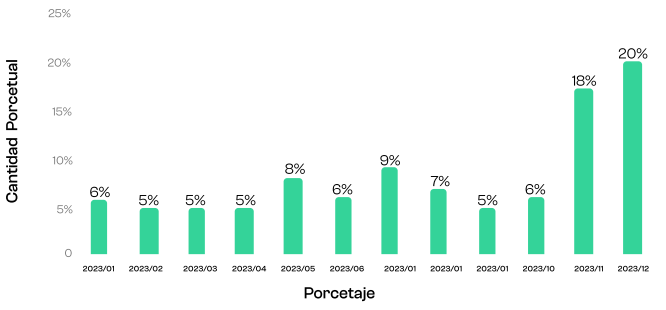
Destaca la aparición de "Hh.exe", herramienta que puede ser usada para descargar archivos mediante la ayuda de un script HTML. De no ser monitoreada, es altamente probable pasar desapercibido en una red interna.



Cantidad Detecciones Lolbas - 2023

Durante los últimos meses de 2023 es notable el aumento del uso de estas herramientas.

Nuevamente, esto es consistente con la información observada en otros gráficos que muestran aumentos sostenidos de grupos y actividad hacia fin de año.



Conclusiones

El número de brechas totales va al alza y cada vez con mayor fuerza, particularmente afectando a Sudamérica. Además de generar impacto en las mismas compañías, se ve afectada la cadena de suministro (proveedores de servicio, infraestructura crítica) creando una cadena de impacto que puede terminar en consecuencias desastrosas. Los actores diferentes van en aumento y, en consecuencia, la variedad de tácticas y técnicas que utilizan para atacar a sus víctimas.

Las vulnerabilidades que afectan transversalmente a todos los sectores (Microsoft Exchange, Log4j, Ivanti, MOVEit, VeeamBackup, ESXi) sirven como vector de entrada a amenazas más avanzadas y al eventual impacto en las operaciones. Su parchado debe ser prioritario dentro de las operaciones de las compañías.

En concordancia con los actores diferentes, tiene relación el uso de diferentes tácticas, técnicas y métodos para poder concretar sus ataques: El phishing y spearphishing para obtener credenciales sigue siendo un elemento común entre los actores de Ransomware, además de una economía "subterránea" en la dark web de acuerdo con el aumento en la compra/venta de credenciales filtradas.

La tendencia a utilizar bibliotecas y programas nativos de los sistemas operativos en ataques es preocupante. Es un cambio sutil pero significativo en las estrategias utilizadas por los actores de amenaza, pues se aprovechan de herramientas usadas en la operación diaria. En consecuencia, la detección y respuesta se torna más desafiante.

A pesar de la sostenida mejora de la capacidad de detección y respuesta de las tecnologías de ciberseguridad, de la creciente madurez del sector en término de profesionales los ataques exitosos siguen creciendo.

De hecho, la amenaza del ransomware se ha convertido en endémica. Las nuevas técnicas y el uso de la IA van a permitir sostener este ritmo. Podemos decir algo parecido del uso de phishing como técnica de acceso inicial.

En el escenario global, se sigue observando a grandes corporaciones, potencialmente maduras, que son víctimas de ataques exitosos de grupos criminales. Es importante tener una explicación sobre porqué, sucede esto. Varias hipótesis son posibles. Por ejemplo, el proceso temprano en la evolución en que se encuentra la región desde servicios gestionados tradicionales hacia servicios del tipo MDR. Otro aspecto es la escasez de profesionales. En las organizaciones de gran tamaño, los aspectos de silos y coordinación han jugado en el pasado más de una mala jugada.

En un contexto de crecimiento de la superficie de ataque, el efecto puede ser bastante negativo. Es interesante tomar notar que hay sectores industriales en Latinoamérica que aún no han sido impactados en la región con la fuerza que lo han sido en el hemisferio norte. Este es el caso de las organizaciones de salud y los municipios.

Podemos prever hacia adelante una sostenida actividad en ingeniería social, y ataques tipo CEO Fraud, derivada de la explotación creciente de las IA y las técnicas de deepfake.

En la medida que las tensiones derivadas por los ejes geopolíticos aumenten, se producirá un natural traspaso de técnicas y conocimientos hacia el mundo de cibercrimen y en la eventualidad que esta actividad baje, una parte de los actores que trabajaron para estados, derivarán a la actividad criminal.

TENDENCIAS
DE LA EXPOSICIÓN

Tendencias de la Exposición

Con el avance de las técnicas y tácticas de ataques, especialmente con la llegada de la inteligencia artificial, las empresas no logran reducir su exposición mediante enfoques tradicionales de gestión de riesgos debido a su naturaleza de realizar análisis aislados y muchas veces poco realistas, centrados excesivamente en las vulnerabilidades y herramientas.

Adicionalmente, los programas de gestión de vulnerabilidades generan informes extensos y complejos de implementar, convirtiendo la misión de proteger de manera preventiva en una tarea ardua y sin fin. Priorizar las medidas de remediación considerando solo la criticidad de la vulnerabilidad ha demostrado ser insuficiente frente al dinamismo de las amenazas y su característica de integrar diversas dimensiones y tácticas de ataque.

Adoptar un programa que complemente la gestión de riesgos con el enfoque de adaptarse continuamente al escenario de amenazas contribuye efectivamente a una postura más proactiva y ágil en un mundo en constante transformación.

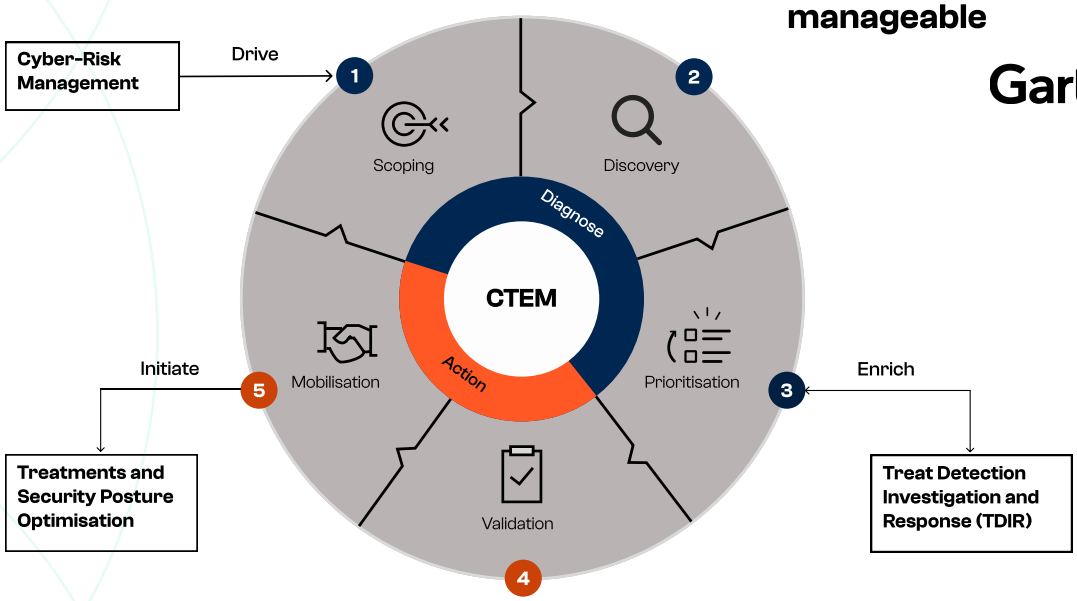
Para ello necesitamos un enfoque más dinámico y realista que gestione continuamente los riesgos y amenazas.

Una visión innovadora con el CTEM

CTEM FRAMEWORK

5 step process make exposure management manageable

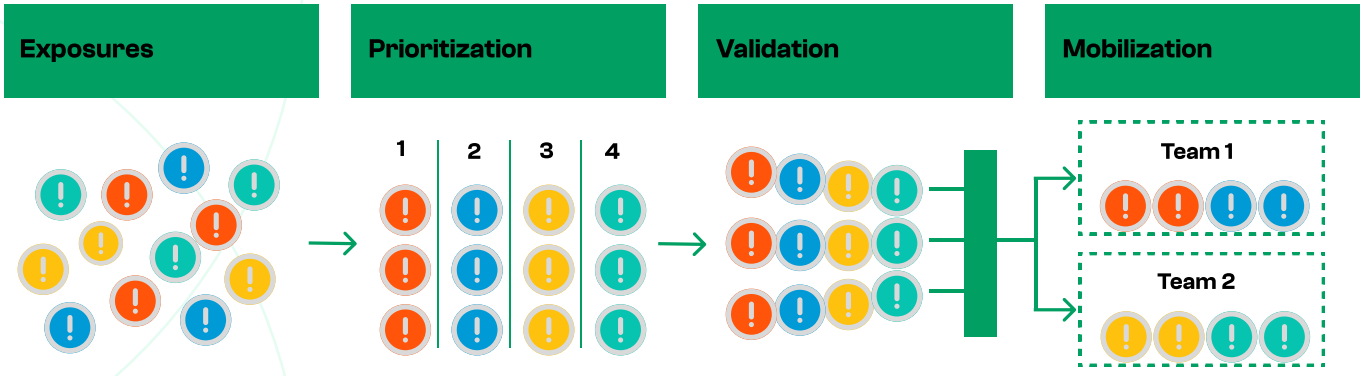
Gartner



Fuente: Gartner, Top Strategic Technology Trends for 2024: Continuous Threat Exposure Management, Jeremy D'Hoinne, Pete Shoard, 16 October 2023

Cómo podemos hacerlo – CTEM

Steps Toward Producing Priotized and Validated Risk Exposures



Explosion in attack surface leads to high volume, unscoped issue identification

Issues are organized into business-driven scopes and prioritized by importance

Validation works as a filter to prove which discovered exposures could actually impact the organization

Prioritized and validated risk exposures are mobilized with the respective teams

Gartner

Fuente: Gartner, 2024 Strategic Roadmap for Managing Threat Exposure, Pete Shoard, 8 November 2023

Nuestra Visión

En nuestra experiencia con más de 800 ejercicios de validación de capas de seguridad, identificamos que las empresas priorizan mal los recursos para proteger sus activos más importantes (las joyas de la corona), debido a su escaso conocimiento de la superficie de ataque.

Con la restricción de recursos de las empresas y ataques cada vez más sofisticados, recomendamos inversiones en la detección y actuación proactiva para reducir la superficie de ataque.

Índice de Exposición

Los clientes con un buen nivel de madurez de Exposición (Hardening) no tuvieron sus **Joyas de la Corona** comprometidas en los ejercicios de explotación (Red Team)

30,8%

Sector Financeiro

Vectores externos:

29
Días de acceso a las plataformas o red (media)

76
Días para escalada de privilegios (media)

60%
Pulverización de contraseñas
(Contraseñas fáciles)

20%
Ingeniería social
(Artefactos maliciosos)

20%
Ingeniería social
(Robo de credenciales)

Vectores Internos:

100%
Osint
(Credenciales en texto claro)

Manufactura

Vectores externos:

29
Días de acceso a las plataformas o red (media)

29,7
Días para escalada de privilegios (media)

45%
Pulverización de contraseñas
(Contraseñas fáciles)

30%
Ingeniería social
(Artefactos maliciosos)

25%
Ingeniería social
(Robo de credenciales)

Vectores Internos:

50%
Osint
(Credenciales en texto claro)

37,5%
Pulverización de contraseñas
(Contraseñas fáciles)

6,2%
Configuración faltante
(Explotaciones de artefactos)

6,2%
Otros

Medios

2

Días de acceso a las plataformas o red (media)

14

Días para escalada de privilegios (media)

Vectores externos:

100%

Pulverización de contraseñas **(Contraseñas fáciles)**

Vectores Internos:

100%

Osint **(Credenciales en texto claro)**

Salud

Vectores externos:

27
Días de acceso a las plataformas o red (media)

26
Días para escalada de privilegios (media)

66,6%
Pulverización de contraseñas
(Contraseñas fáciles)

33,4%
Ingeniería social
(Robo de credenciales)

Vectores Internos:

42,8%
Pulverización de contraseñas
(Contraseñas fáciles)

28,5%
Osint
(Credenciales en texto claro)

14,5%
Configuración faltante
(Explotaciones de artefactos)

14,2%
Otros

Servicios

18
Días de acceso a las plataformas o red (media)

25,4
Días para escalada de privilegios (media)

Vectores externos:

45%
Pulverización de contraseñas
(Contraseñas fáciles)

30%
Ingeniería social
(Artefactos maliciosos)

20%
Ingeniería social
(Robo de credenciales)

5%
Osint
(Datos expuestos)

Vectores Internos:

50%
Osint
(Credenciales en texto claro)

25%
Pulverización de contraseñas
(Contraseñas fáciles)

18,7%
Configuración faltante
(Explotaciones de artefactos)

6,3%
Otros

Retail

13
Días de acceso a las plataformas o red (media)

28,5
Días para escalada de privilegios (media)

Vectores externos:

55,5%
Pulverización de contraseñas
(Contraseñas fáciles)

33,3%
Ingeniería social
(Artefactos maliciosos)

11,2%
Ingeniería social
(Robo de credenciales)

Vectores Internos:

50%
Pulverización de contraseñas
(Contraseñas fáciles)

25%
Configuración faltante
(Explotaciones de artefactos)

12,5%
Osint
(Credenciales en texto claro)

12,5%
Otros

Principales Debilidades

Listado de las vulnerabilidades explotadas el 2023 en campañas conocidas de Ransomware

CVE	VENDOR	PRODUCTO	LATAM	TÉCNICA MITRE ATT&CK
CVE-2022-41080	Microsoft	Exchange Server	SI	T1190: Exploit Public-Facing Application
CVE-2022-47966	Zoho	ManageEngine	SI	T1190: Exploit Public-Facing Application
CVE-2017-11357	Telerik	User Interface (UI) for ASP.NET AJAX	SI	T1190: Exploit Public-Facing Application
CVE-2022-21587	Oracle	E-Business Suite	SI	T1190: Exploit Public-Facing Application
CVE-2022-24990	TerraMaster	TerraMaster OS	SI	T1190: Exploit Public-Facing Application
CVE-2023-0669	Fortra	GoAnywhere MFT	SI	T1190: Exploit Public-Facing Application
CVE-2022-47986	IBM	Aspera Faspex	SI	T1190: Exploit Public-Facing Application
CVE-2022-41223	Mitel	MiVoice Connect	NO	T1190: Exploit Public-Facing Application
CVE-2022-40765	Mitel	MiVoice Connect	NO	T1190: Exploit Public-Facing Application
CVE-2022-36537	ZK Framework	AuUploader	NO	T1190: Exploit Public-Facing Application
CVE-2017-7494	Samba	Samba	SI	T1190: Exploit Public-Facing Application
CVE-2021-27876	Veritas	Backup Exec Agent	SI	T1190: Exploit Public-Facing Application
CVE-2021-27877	Veritas	Backup Exec Agent	SI	T1190: Exploit Public-Facing Application
CVE-2021-27878	Veritas	Backup Exec Agent	SI	T1190: Exploit Public-Facing Application
CVE-2023-27350	Paper Cut	MF/NG	SI	T1190: Exploit Public-Facing Application
CVE-2021-45046	Apache	Log4j2	SI	T1190: Exploit Public-Facing Application
CVE-2023-34362	Progress	MOVEit Transfer	SI	T1190: Exploit Public-Facing Application
CVE-2022-31199	Netwrix	Auditor	NO	T1190: Exploit Public-Facing Application
CVE-2023-3519	Citrix	NetScaler ADC and NetScaler Gateway	SI	T1190: Exploit Public-Facing Application
CVE-2023-35078	Ivanti	Endpoint Manager Mobile (EPMM)	NO	T1190: Exploit Public-Facing Application
CVE-2023-27532	Veeam	Backup & Replication	SI	T1190: Exploit Public-Facing Application
CVE-2023-20269	Cisco	Adaptive Security Appliance and Firepower	SI	T1190: Exploit Public-Facing Application
CVE-2023-42793	Jet Brains	TeamCity	SI	T1190: Exploit Public-Facing Application
CVE-2023-22515	Atlassin	Confluence Data Center and Server	SI	T1190: Exploit Public-Facing Application
CVE-2023-40044	Progress	WS_FTP Server	NO	T1190: Exploit Public-Facing Application
CVE-2023-4966	Citrix	NetScaler ADC and NetScaler Gateway	SI	T1190: Exploit Public-Facing Application
CVE-2023-46604	Apache	ActiveMQ	SI	T1190: Exploit Public-Facing Application
CVE-2023-22518	Atlassian	Confluence Data Center and Server	SI	T1190: Exploit Public-Facing Application
CVE-2023-41266	Qlik	Sense	SI	T1190: Exploit Public-Facing Application
CVE-2023-41265	Qlik	Sense	SI	T1190: Exploit Public-Facing Application
CVE-2023-24880	Microsoft	Windows	SI	T1566: Phishing
CVE-2019-1388	Microsoft	Windows	SI	T1566: Phishing
CVE-2023-28252	Microsoft	Windows	SI	T1566: Phishing
CVE-2023-36884	Microsoft	Windows	SI	T1566: Phishing
CVE-2023-33831	RARLAB	WinRAR	SI	T1566: Phishing

Un 86% de las vulnerabilidades explotadas por actores de amenaza de Ransomware corresponden a dispositivos expuestos a Internet.

En un 14% los actores de amenazas de Ransomware utilizan Phishing para explotar vulnerabilidades en estaciones de trabajo.

Cerca de un 83% de las vulnerabilidades explotadas corresponden a dispositivos o software que se encuentran en LATAM y el resto del mundo.

Un 46% de las vulnerabilidades explotadas corresponden a fallas del año 2022 o anteriores.

Debilidades en la Nube

AWS

Top 10 Vulnerabilidades (del 01.01.2023 al 31.12.2023)	Cantidad de Vulnerabilidades encontradas	Cantidad de Evaluaciones ejecutadas
Ensure routing tables for VPC peering are "least access"	25.337.530	61.594
Check if EBS snapshots are encrypted	7.156.627	61.594
Unencrypted EC2 AMIs	1.892.231	61.594
S3 buckets without MFA Delete policy	1.881.937	61.594
Check if Lambda functions invoke API operations are being recorded by CloudTrail	1.880.223	61.594
Check if S3 buckets have policy to enforce security encryption	1.875.770	61.594
Check if S3 buckets have transport encryption enabled and policy to enforce it	1.764.873	61.594
Check if S3 buckets have Object-level logging enabled	1.726.815	61.594
Check if S3 buckets have server access logging enabled	1.725.328	61.594
Check if SQS queues have encryption enabled	1.716.452	61.594

Azure

Top 10 Vulnerabilidades (del 01.01.2023 al 31.12.2023)	Cantidad de Vulnerabilidades encontradas	Cantidad de Evaluaciones ejecutadas
Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it	3.620.515	29.200
Ensure that a 'Diagnostic Setting' exists	3.475.093	29.200
Ensure that standard pricing tier is selected	470.884	29.200
Ensure that 'Storage Encryption' is set to 'On'	367.409	29.200
Ensure that 'SQL Encryption' is set to 'On'	363.402	29.200
Ensure that 'SQL auditing & Threat detection' is set to 'On'	363.389	29.200
Ensure that 'Vulnerability assessment' is set to 'On'	347.571	29.200
Ensure that 'Network security groups' is set to 'On'	341.154	29.200
Ensure that 'Web application firewall' is set to 'On'	340.323	29.200
Ensure that Resource Locks are set for Mission-Critical Azure Resources	271.677	29.200

Google

Top 10 Vulnerabilidades (del 01.01.2023 al 31.12.2023)	Cantidad de Vulnerabilidades encontradas	Cantidad de Evaluaciones ejecutadas
Ensure BigQuery dataset is encrypted with customer-managed encryption keys (CMEK)	625.972	2.316
Ensure that storage bucket logging is enabled	309.557	2.316
Ensure that Cloud Storage bucket is encrypted with customer-managed encryption keys (CMEK)	308.725	2.316
Ensure that Cloud Storage buckets have uniform bucket-level access enabled	303.949	2.316
Ensure that VPC Flow Logs is enabled for every subnet in a VPC Network	106.683	2.316
Ensure Private Google Access is set on Subnets	105.584	2.316
Ensure that there are only GCP-managed service account keys for each service account	19.967	2.316
Ensure user-managed/external keys for service accounts are rotated every 90 days or less	18.056	2.316
Ensure that firewalls logging are enabled	17.981	2.316
Ensure that Firewall access is restricted from the internet	15.554	2.316

Conclusiones y recomendaciones:

Implementar un enfoque más proactivo, dinámico y que se adapte rápidamente a las amenazas, es necesario para la efectiva construcción de resiliencia con capas efectivas de protección.

La reducción progresiva del tiempo de detección y permanencia de una amenaza en el ambiente son indicadores fundamentales para la maduración de la postura y eficacia de los controles.

Buscar la disminución de la superficie de riesgos a través de controles preventivos (hardening), dificultando los caminos de movimientos laterales y la escaladas de privilegios, impone un alto costo para llevar a cabo un ataque dirigido, proporcionando una parte fundamental de la estrategia de resiliencia.

TENDENCIAS
DE LA INDUSTRIA

1

Deepfake, cuando nos robaron el rostro

Deepfake, cuando nos robaron el rostro

La capacidad de autenticar una identidad se basa en tres elementos: algo que sabemos, algo que tenemos y algo que somos. El “algo que somos” es lo que se encuentra más cerca a nuestra propia percepción de identidad y es algo que no podemos modificar y es por lo que, generalmente, los otros seres humanos nos reconocen y autentican. Si bien el “algo que somos”, tiene múltiples facetas (nuestra voz, nuestro rostro, una huella, la marca de calor de nuestro rostro, nuestro ADN, etc.) la cotidianeidad de la autenticación está asociada a nuestro rostro y nuestra voz.

La prueba de vida, es decir escuchar a una persona, verla e interactuar con ella, ha sido uno de los mecanismos más confiables para confirmar una identidad. Los rápidos desarrollos en las calidades y herramientas de edición, generación de video, voz, y por sobre todo el desarrollo de IA, que es capaz de generar videos realistas, son un fuerte golpe a este mecanisimo de autenticación.

La capacidad de las IA de "sintetizar la identidad" con una experiencia cercana a lo real, posibilitando engañar tanto a personas como a algoritmos, es una técnica que está al alcance de muchos y está dando lugar al fenómeno denominado “deepfake”. El deepfake ya ha logrado éxitos como instrumento de la amenaza cibernética, engañando en algunas ocasiones a personas y en otras a algunos sistemas de autenticación a través de las llamadas “pruebas de vida”.

El deepfake tiene una faceta aún más oscura cuando sumamos el potencial masivo otorgado por las redes sociales y la capacidad de las IA de aprender estilos de lenguaje y por tanto imitar personalidades. El deepfake no es sólo un problema de criminalidad, sino que puede devenir en un problema político al manipular masivamente a grandes segmentos de la sociedad. La industria está buscando mecanismos para enfrentar el problema y también los legisladores. El impacto que puede provocar este nuevo tipo de amenaza puede ser de magnitudes inimaginables, como bien señala Yuval Harari (ver video “AI & the future of humanity” en YouTube).

Las posibilidades de detección de deepfakes bien ejecutados por parte de seres humanos es baja. Si se trata de imágenes o videos, algunas cosas que pueden indicar un deepfake son incongruencias en la piel, sombras alrededor de los ojos, barba poco reales, o movimientos poco realistas, pero es complejo poder prestar atención a esas cosas en el medio de una conversación. En el caso de los sonidos, la nitidez de la voz puede ser un punto por considerar para determinar si lo que estamos escuchando es un deepfake o no, junto con la coincidencia con el movimiento de los labios si es un video.

Herramientas de reconocimiento facial también podrían ser “burladas” por imágenes generadas por IA, aunque varias tecnologías modernas, como FaceID de Apple, son capaces de detectar la "profundidad" de la cara mediante infrarrojo, la distancia a los diversos puntos de la cara, y eso hace que no sea posible realizar el desbloqueo de un equipo mediante una foto generada por IA.

Una parte de los controles para esta amenaza, provendrán de sistemas que sean capaces de detectar tanto videos como voces falsas. Así como las IA, son las herramientas requeridas para crear deepfakes, también son las que proveen diversos métodos para poder detectarlas. Debiéramos esperar que muchas de estas capacidades sean incorporadas de manera nativa a las plataformas de video-conferencia y sean parte de las funcionalidades básicas de las mismas.

Pero si el problema se está dando en el ámbito de “algo que somos”, para asegurar la identidad, tendremos que recurrir a “algo que tenemos” o “algo que sabemos”. La inclusión de mecanismos de certificados, firma digital, token u otros debieran complementar la presencia virtual (video y voz). La profundización de “algo que somos” también puede ser una opción, usando huella digital u otros patrones. Posiblemente, esto va a generar toda una industria de robar los variados aspectos de “algo que somos”.

La forma en que se abordan los procesos más críticos como la necesidad autorizaciones adicionales, podrían limitar el espacio de acción de los delincuentes, al menos a nivel corporativo.

La segregación de funciones es una herramienta ya existente que también aportará un nivel adicional de control.

El escenario en el mundo de los individuos privados es más complejo. La interacción habitual entre familiares y amistades suelen tener elementos de confianza y la prueba de vida es suficiente.

Acá se dependerá de la evolución de los sistemas por dónde interactúan las personas para que incorporen nuevos mecanismos de detección de deepfake.

Por supuesto, la educación y el awareness pasan a ser un elemento relevante. Es de especial relevancia la presencia de factores culturales de algunas organizaciones, donde las jefaturas promueven un bypass de los protocolos para obtener mejores tiempos de respuesta. Estas son vulnerabilidades que en el pasado han sido utilizadas por los ataques tipo CEO Fraud y que con el deepfake encuentran un espacio promisorio.

Recomendaciones NeoSecure by SEK:

- **Realizar una evaluación de riesgo derivado del deepfake para identificar en qué procesos puede generar más impacto.**
- **Ver cuáles de estos procesos pueden ser ejecutados a través de sistemas incorporando un factor de autenticación adicional**
- **Analizar qué procesos críticos pueden ser condicionados a la aprobación de dos personas.**
- **Analizar la limitación de privilegios a fin de limitar el impacto de una acción agresiva.**
- **Evaluar sistemas de prueba de vida robustos para ser aplicados a nivel interno y de clientes.**
- **Iniciar un proceso de concientización y educación de cara a la organización para prevenir esta amenaza.**

IA también es un sistema a ser protegido

IA también es un sistema a ser protegido

Son cada vez más las organizaciones que están trabajando para poder beneficiarse de las capacidades de las IA, y por lo tanto incorporarlos dentro de su ecosistema. Los sistemas de IA, con todas sus capacidades, son un recurso más, dentro de una larga lista, que deben ser protegidos.

Ya se han identificado una serie de amenazas específicas a los sistemas de IA, que están orientadas, por ejemplo, a envenenar los datos, y lograr de ellos comportamientos inesperados, como que entreguen información que no debieran entregar. Sin embargo, como sistemas de información, los sistemas de IA cuentan también con repositorios de datos, infraestructura sobre la que operan, código aplicativo y los elementos comunes a todos los sistemas. Es por eso que una estrategia integral de protección de los sistemas de IA, debe incorporar también la protección de los elementos más tradicionales.

Para esto, se deben proteger sus tres componentes principales: los datos (orígenes de datos utilizados para entrenar el modelo), el modelo (diferentes algoritmos de AI) y el uso (inferencia de la IA). La industria ya está proponiendo algunos frameworks de protección de las IA (Gartner entre otras organizaciones ya cuenta con uno), que buscan modelar de forma integral los componentes arriba mencionados y sus controles.

Los datos utilizados para el modelo podrán ser susceptibles de envenenamiento (que afectará la exactitud de las inferencias, por incorporar datos inexactos o falsos en el origen de datos que luego vayan a pasar por el proceso de modelado), o de exfiltración/fuga (que significará una violación de la privacidad de estos, ya que para aumentar la exactitud de las respuestas de la IA, muchas veces serán utilizados datos sensibles para alimentarla). Para proteger los orígenes de datos de nuestra IA de esta amenaza, utilizaremos los métodos tradicionales de protección de datos: descubrimiento/clasificación, criptografía, control de accesos, y monitoreo.

En cuanto al modelo, la mayoría de las veces se usarán modelos abiertos, por lo que, como cualquier otra cadena de suministro, habrá que ser muy riguroso respecto a la autenticidad de los orígenes desde los cuales dichos modelos se consuman. Si los modelos son operados/consumidos a través de API, dicha exposición del modelo deberá tener los controles de seguridad correspondientes. Habrá que tener especial atención también con lo que se refiere a la propiedad intelectual de los datos con los que se alimenten los modelos, para evitar problemas legales. La protección de nuestro modelo deberá llevarse a cabo mediante la hardenización del acceso al mismo (RBAC, mínimos privilegios, control de orígenes, etc.).

Por último, proteger el uso de la IA de los ataques más comunes hoy en día sobre estos, detallados en OWASP Top 10 for LLM Applications, https://owasp.org/www-project-top-10-for-large-language-model-applications/, de los cuales podemos destacar Prompt Injection, Model Denial of Service, o Model Theft, entre otros.

En los últimos años, han surgido soluciones tecnológicas de Machine Learning Detection and Response, MLDR, tales como por ejemplo HiddenLayer, https://hiddenlayer.com/, o soluciones de monitoreo específicas de ML, tales como WhyLabs, https://whylabs.ai/, que simplifican los controles y el monitoreo sobre IA, y ofrecen diversos controles de integridad sobre las mismas.

Recomendaciones NeoSecure by SEK:

- **Evaluar con cuidado los posibles riesgos que presentaría el uso de estas aplicaciones de IA dentro de la organización, para así determinar las prioridades de protección.**
- **Estudiar algún modelo integral de protección de las IA para ayudar a identificar riesgos potenciales y definir una estrategia de protección.**
- **Uso de controles específicamente dirigidos a el nuevo tipo de riesgos que posee una IA, tales como Pentesting específicos para IA.**

Automatización, más allá del SOAR

Automatización, más allá del SOAR

Automatización sigue siendo una palabra sumamente atractiva, pues presupone reemplazar una enorme cantidad de pasos manuales por un workflow automatizado con mínima o nula intervención de un ser humano. El resultado esperado de esto será siempre una menor cantidad de recursos humanos, menor cantidad de tiempo para cumplir un proceso, y un margen de error mucho más bajo o casi nulo.

En ciberseguridad, el SOAR ha sido durante los últimos años el sinónimo de automatización, pasando de ser un conjunto de playbooks aislados encargados de realizar la atención de incidentes de seguridad de baja/mediana criticidad, a convertirse en el orquestador central de una gran cantidad de tareas de tecnología relacionadas con Seguridad.

Sin embargo, la automatización no es una invención de ciberseguridad y aún el mismo SOAR es una versión especializada de los antiguos workflows hoy devenidos en BPMs. Aún más, la automatización no acaba en el SOAR, y existe un gran espacio dónde automatizar fuera de su alcance. Numerosas tecnologías han asumido esa tarea para los ambientes de SecDevOps, parchado, integración de plataformas y otros.

La industria de TI ha desarrollado por años diversas prácticas y miradas en torno a la automatización, las que con el advenimiento de la ola de transformación digital se profundizaron.

Se ha usado la combinación de herramientas de IA/ML y RPA, habilitando la automatización para casi cualquier tarea repetitiva ejecutada, buscando producir una total transformación digital. Estos modelos, prácticas y herramientas han madurado en paralelo al desarrollo de la industria de ciberseguridad. Si consideramos que hoy la ciberseguridad se encuentra embebida en diversos ambientes, como aplicaciones, redes, nube, DevOps, es natural pensar en cómo utilizar ese know-how para acelerar la tarea de automatización de los procesos ciberseguridad.

Recomendaciones NeoSecure by SEK:

- **Comprender el alcance de las diferentes herramientas disponibles en el entorno de ciberseguridad para lograr automatizar, particularmente las herramientas de SOAR.**
- **Crear los casos de negocio, basados en ahorro en tiempo, disminución de impacto y ahorro de horas de personal especializado.**
- **Estudiar las estrategias de automatización usadas por los equipos de transformación digital y sus formas de presentar frente al negocio esos casos para maximizar la factibilidad de los mismos. Recomendamos analizar las implicancias de seguridad al crear estos sistemas de automatización de los propios procesos de ciberseguridad.**

Seguridad de la Identidad,
no sólo prevenir, también detectar

Seguridad de la Identidad, no sólo prevenir, también detectar

"La identidad es el perímetro" repite el mantra que busca poner a este aspecto de la ciberseguridad en el lugar relevante que debe tener y es de hecho el gran punto de partida en la construcción de una organización segura. La identidad es la que abre las puertas del reino y es por eso por lo que la robustez de esta es esencial.

La raíz de la seguridad de la identidad tiene su origen en el foco que ponen en ella los actores maliciosos. La identidad es robada a través de métodos de ingeniería social o a través de otros mecanismos más sofisticados con ataques variados que incluyen desde los ataques del tipo Man In The Middle a ataques del tipo Golden Ticket. El control de la identidad es un gran pasaporte a toda clase de accesos y privilegios y es por eso que la cantidad de técnicas de ataque y variantes de las mismas dirigidas a obtenerla sigue creciendo, incluidos los nuevos ataques de deepfake ya mencionados en este documento.

Es por esto uno de los espacios dónde aparecen los controles más antiguos de seguridad tales como la contraseña y la limitación de accesos. Desde ese inicio hasta el presente, para proteger la identidad se han venido sofisticando los controles y han surgido variadas opciones de estos: sistemas de autenticación múltiples, sistemas biometricos, autenticación basada en comportamiento, autenticación privilegiada, firma digital, certificados, almacenamiento de certificados seguros, etc.

El desarrollo conceptual de modelos y estrategias en ciberseguridad, han llevado a idear estrategias como las basadas en el modelo Zero Trust, dónde la identidad es central: identificar permanentemente sesiones, identificación basada en riesgo, limitar acceso sólo a lo requerido, son algunas de las ideas centrales de este modelo, que parece a ratos un desarrollo amplificado de los conocidos principios de "need to know" y "least privilege", aun cuando contiene aportes originales y complementarios.

Sin embargo, la aplicación de una estrategia de Zero Trust tampoco ha estado ajena a dificultades. Estas nacen de la creciente complejidad de los ambientes de TI y sus interacciones internas y externas. La sola idea de poder mantener una lista de privilegios actualizada en una organización parece una quimera por los cientos de sistemas, miles de personas, roles variados, cambios internos, desvinculaciones, contrataciones y otros. En estos ambientes, la implementación de sistemas de gestión de las identidades o la simple adopción de sistemas robustos de autenticación pueden significar proyectos complejos o levantar oposición interna.

En este escenario, el cuidado de la identidad debe ser auxiliado por otros tipos de controles, que nos permitan detectar cuándo éstas fueron robadas. Los sistemas de UEBA han venido cumplimiento esta función desde hace un tiempo, aun cuando su adopción ha sido lenta.

Gracias a estos sistemas, se puede establecer una capa de control que cubra lo que por uno u otro motivo no se ha cubierto. La posibilidad de poder identificar comportamientos anómalos o claramente agresivos es un control necesario, no sólo para detectar el robo vulgar de identidad a través de ingeniería social, sino también para detectar los robos de identidad más sofisticados, producidos a partir de técnicas más elaboradas, como los ataques del tipo Golden Ticket o Pass The Hash. Esta es entonces una pieza del modelo Zero Trust que complementa los controles de identificación, autenticación y control de acceso.

Recomendaciones NeoSecure by SEK:

- **Complementar las estrategias de protección de identidad a través de la implementación de sistemas de monitoreo, que permitan identificar intentos de robo de identidad o comportamientos anómalos que puedan señalar una identidad ya robada.**
- **Evaluar sistemas de User and and Entity Behavior Analytics y sus diversos casos de uso que permitan monitorear no solo la actividad de usuarios en diversos ambientes (on-premise, cloud, OT, etc.) sino también de las diversas "máquinas" o sistemas que pudieran ser atacadas para aprovechar sus accesos.**
- **Integrar estos sistemas a otros (EDR, NDR) que permitan identificar ataques dirigidos, dónde el robo de identidad es parte de las estrategias para escalar privilegios o lograr movimiento lateral.**

Más allá de la gestión de vulnerabilidades: La Gestión Continua de la Exposición

Más allá de la gestión de vulnerabilidades: La Gestión Continua de la Exposición

En los lejanos días de la industria, la letanía de "elimina las vulnerabilidades y estarás seguro" era repetida de manera incansable por el naciente mundo de profesionales de ciberseguridad. Había y hay razón en hacerlo, porque el parchado sigue siendo uno de los controles más efectivos para evitar que una vulnerabilidad sea explotada y un atacante gane acceso o genere una denegación. Sin embargo, a pesar de la persistencia y los esfuerzos, la tarea de parchar se fue haciendo sostenidamente más difícil.

En el proceso, surgieron sistemas de descubrimiento de vulnerabilidades y de parchado automático, se mejoraron los procesos para priorizar, y se aumentaron las plantillas de personas que parchaban.

Aun así, el problema eludió los esfuerzos. Ataques tan relevantes como el de OPM o Equifax tuvieron en el centro de sus causas la mala gestión de la superficie del ataque y sus impactos a el negocio. Con el tiempo, el problema se fue camuflando como un problema eminentemente operativo: una cola de sistemas por parchar y la lucha por vaciarla.

Adicionalmente, el crecimiento sostenido y a veces acelerado de la superficie de ataque, creó ámbitos nuevos y desconocidos, los que no pocas veces quedan fuera del ámbito de los equipos operativos de parchado.

Hoy la industria propone una mirada amplia e integral al fenómeno a través del concepto de Gestión Continua de la Exposición a Amenazas (Continuous Threat Exposure Management o CTEM).

Esta mirada considera variados aspectos. El primero, es relacionar la tarea de la gestión de la exposición con los riesgos del negocio. Esta mirada es necesaria como punto de partida de la priorización, y también de la identificación de aquellas superficies de ataque que son más sensibles.

El segundo aspecto es relacionar la perspectiva de la exposición a la perspectiva de la amenaza, es decir analizar como los sistemas responden frente a la acción agresiva de los adversarios. La incorporación de las técnicas avanzadas de Red Team, cómo ingeniería social, son algunos de los elementos que enriquecen esta perspectiva. Un tercer aspecto es integrar los diversos ambientes, (red interna, nube, datos expuestos en sistemas SaaS) para tener una visión global.

Como cuarto aspecto se encuentra la integración de diversas técnicas y/o herramientas de detección de exposición, en superficies on premises y nube, para poder así tener la visión integrada de la exposición.

La integración de todas estas perspectivas, permitirán tener un punto único de control de la exposición y así priorizar adecuadamente el esfuerzo de mitigación. Por supuesto el esfuerzo de mitigación es la continuación de todo el proceso de descubrimiento y priorización.

Recomendaciones NeoSecure by SEK:

- **Delinear una estrategia de CTEM que considere un roadmap que empiece con la fase de descubrimiento, para saber cuál es es esfuerzo y presupuesto necesario para lograr los objetivos de la empresa, con una camada de servicio, para vincular las diversas exposiciones al negocio y a la gestión de riesgos**
- **Analizar desde ahí las estrategias de priorización de la mitigación**

Para esa estrategia recomendamos el **Business Takeover Simulation**, una oferta exclusiva de NeoSecure by SEK, para lograr los primeros pasos del CTEM, con un producto de seguridad ofensiva continuo desde la perspectiva del atacante.

El Next Generation CISO

El Next Generation CISO

Los diversos cambios en el medio han transformado los focos de variados roles profesionales y el CISO no es la excepción. En la medida que el impacto de la amenaza y los presupuestos de ciberseguridad han crecido, el cargo de CISO ha venido ganando espacio en el entorno corporativo a través del tiempo y su rol ha venido cambiando.

El CISO enfrenta nuevos desafíos, todos ellos menos técnicos y más ligados al negocio. Así, el CISO debe desarrollar facetas variadas. Hemos identificado la faceta de estratega, de orquestador de diversos equipos, de comunicador interno y externo, de optimizador y de habilitador, como algunas de las facetas claves que el CISO debe buscar desarrollar.

El CISO como estratega deberá entender las diferentes opciones que enfrentar para cumplir los objetivos de la organización. Se enfrenta a diversos conceptos y modelos de seguridad que deberá comprender y a través de su comprensión fijar un camino.

Qué tipo de acciones debe llevar a cabo para lograr una organización más resiliente, qué estrategias seguir para lograr una mejor capacidad de detección y respuesta con menores recursos, en qué tipo de controles poner el énfasis. Son variadas las preguntas que requieren de una mirada global que permita definir un camino de largo plazo.

El CISO como orquestador tiene que entenderse con diversas grupos internos y externos para conseguir que los objetivos de estos estén alineados con los propios, que debieran ser a su vez los del negocio. Así, por ejemplo, debe buscar que los sistemas de la organización sean seguros desde el origen, es decir desde que son diseñados y desarrollados. Debe para esto lograr que estas prácticas se establezcan en los equipos de desarrollo, los que son medidos por métricas de productividad y no de seguridad. Debe conseguir que la cadena de valor eleve sus niveles de seguridad, limitando así las posibilidades de que un ataque provenga desde ahí.

Esto lo llevará a interactuar con actores externos que tienen otras prioridades y urgencias. Debe lograr que los equipos de infraestructura diseñen sus sistemas pensando en la resiliencia, minimizando así el impacto de un ataque. En general, deberá orquestar la acción de diversos equipos logrando que los objetivos mutuos estén alineados y especialmente en organizaciones complejas, esta tarea será cada vez más esencial.

El CISO como comunicador debe poder explicar al negocio, en los términos de éste, los riesgos y la justificación de los presupuestos, así como la necesidad de ciertos proyectos y el apoyo para que otras áreas de la organización hagan suyas iniciativas de seguridad y resiliencia.

Debe lograr comunicar a la organización que cada uno es un actor relevante en la cadena de protección y que el ataque comienza por el eslabón más débil, debe comunicar al equipo las necesidades del negocio y las siempre presentes restricciones financieras que podrían causar frustración.

El CISO como comunicador, será un agente de confianza para el medio, explicando cómo la organización cuenta con los planes y resguardos que el mercado requiere. El CISO como comunicador, podría tener su prueba de fuego durante una crisis derivada de un incidente, pues ahí sus palabras serán escrutadas a la luz pública.

El CISO debe ser un optimizador. Debe entender que, si bien está en época de vacas gordas, dónde sus presupuestos crecen, todo gran poder viene con gran responsabilidad. Se le va a pedir que muestre cómo su organización es cada vez más eficaz y cada vez más y eficiente y se le va a pedir sostenidamente que haga eso con cada vez menos dinero. Va a tener que generar para eso iniciativas de automatización, revisión de procesos, externalización, consolidación de tecnologías, negociación de precios, etc.

Y todo esto aumentando a su vez la eficacia, detectando y respondiendo mejor y más rápido, previniendo cada vez más.

El CISO como habilitador, deberá moverse a la velocidad del negocio, sin dar razones para que se lo esquive por ser la fuente permanente de objeciones, retrasos y problemas. Debe conversar con el negocio para diseñar las mejores opciones de cara a los clientes, protegiendo por un lado y facilitando por el otro. Esto supone entendimientos y conversaciones que permitan contar con acuerdos para que la seguridad fluya con los nuevos desarrollos, los nuevos productos, los nuevos ambientes, los nuevos procesos y las nuevas implementaciones.

Recomendacion NeoSecure by SEK:

- **El CISO deberá desarrollar estas nuevas facetas e incorporar dentro de su equipo roles que complementen las capacidades faltantes.**

Conclusiones finales

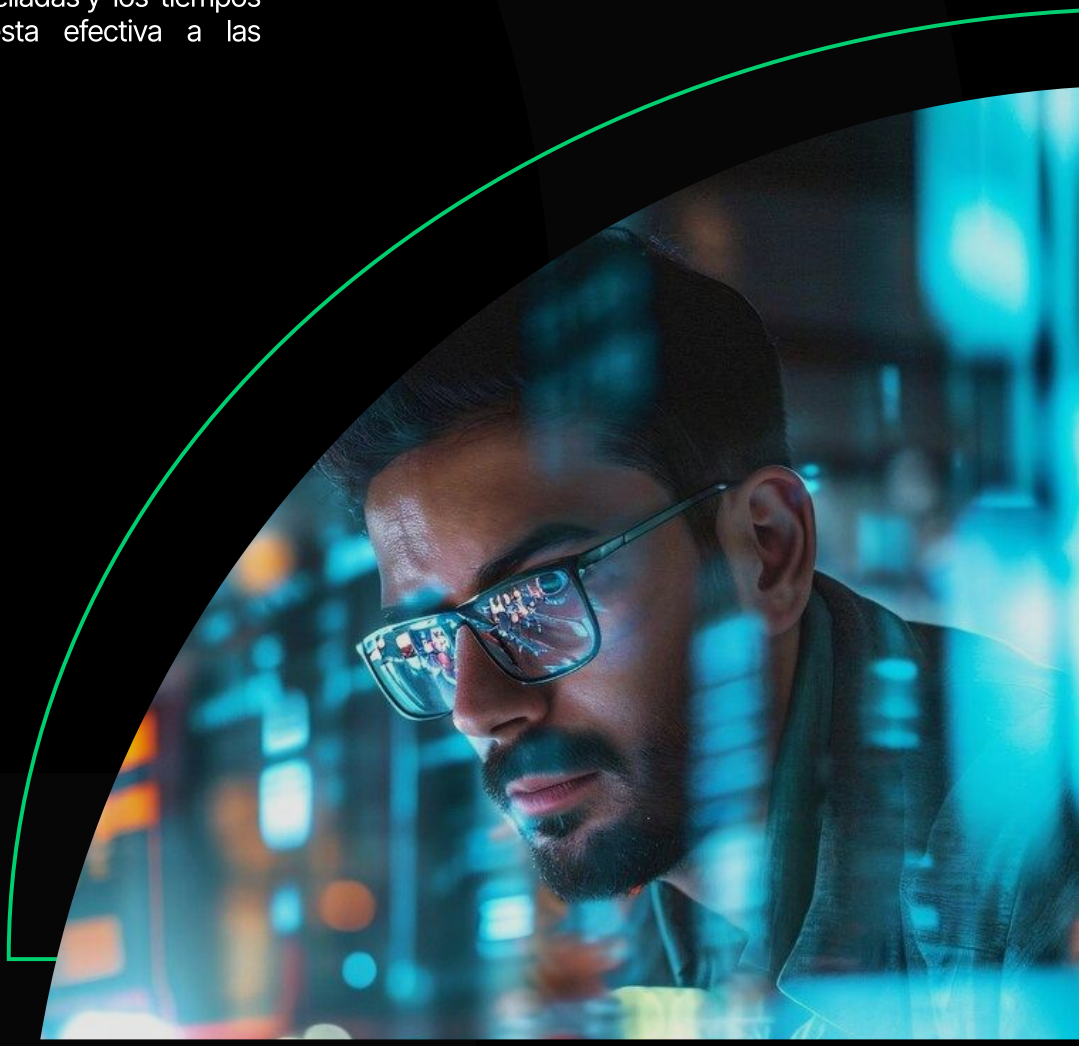
El 2023 ha sido un año donde la amenaza ha crecido y se ha establecido como una realidad presente. No fue un año espectacular, tal vez debido a que los años anteriores habían sido años de cruzar fronteras. Este año comenzamos a cruzar la frontera de la IA, tanto como factor de la amenaza como de factor de la protección.

Vemos operando en la región a una gran cantidad de las grandes organizaciones cibercriminales, y el contexto geopolítico sólo va a profundizar la presencia de estos grupos.

La exposición se complejiza por el crecimiento de la superficie de ataque y los datos recogidos por nuestros equipos de Seguridad Ofensiva, muestran cómo las organizaciones siguen teniendo problemas para mantener sus fronteras selladas y los tiempos para detectar y dar respuesta efectiva a las amenazas continúan muy lejos.

El desafío de los responsables de la seguridad, es cada vez mayor: proteger frente a actores cada vez más evolucionados; orquestar áreas, proveedores y socios de negocios; ser eficiente y efectivo; comunicar y muchos otros. El CISO técnico es cada vez más un recuerdo.

En este escenario, son muchas las tendencias que se puede destacar. Hemos optado por dar algunos énfasis: prepararnos para el deepfake; pensar la automatización más allá del SOAR, comenzar a pensar como vamos a proteger a nuestra propias IAs; complementar con la detección la seguridad de las identidades; iniciar el camino hacia una gestión de la exposición proactiva reduciendo la superficie de riesgo y finalmente, desarrollar nuevas capacidades de gestión, el Next Generation CISO.



NUESTRA VISIÓN

NEOSECURE By SEK Security Ecosystem Knowledge

Por medio de un portafolio de

PRODUCTOS & SERVICIOS

integrados en 4 frentes:

STRATEGY & RISK

Definir la estrategia y el roadmap para inversiones en ciberseguridad, capacitación y consultoría en gobernanza, riesgo y cumplimiento.

- **Assessments**
- **Policies & Plans**
- **Third Party Risk Mang**
- **Education**

EXPOSURE MANAGEMENT

Evaluar/remediar/probar/validar la exposición a vulnerabilidades internas y externas y la eficacia de los controles y operaciones de seguridad.

- **Business Takeover Simulation**
- **Posture Managment**
- **Remediation**
- **Cloud Exposure Managment**
- **Pent Test**

TECHNOLOGY SOLUTIONS

Integración de tecnologías para proteger superficies de ataque.

- **Security Operation**
- **EDR/XDR**
- **Cloud / SASE**
- **Identity Security**
- **OT & IoT Cybersecurity**

MANAGED SERVICES

Servicios recurrentes de monitoreo, administración y respuesta a incidentes en torno a plataformas de seguridad de los clientes.

- **SOC**
- **MDR**
- **Threat Intell**
- **Incident Response**

NeoSecure by SEK reúne soluciones de **ciberseguridad y expertise**

que transforman la estrategia en **protección efectiva**, ofreciendo una jornada integral alineada con los **riesgos, amenazasy madurez** de su negocio

sek.io

THINK AHEAD
REPORT